Math 817 and 818 Notes

Fall 2018 – Spring 2019

Contents

Chapter 1

Group Theory

August 20, 2018

1.1 Definition and first examples

Definition 1.1. A *binary operation* on a set S is a function

$$- \cdot - : S \times S \to S, \text{ given by } (x, y) \mapsto x \cdot y.$$

Remark. We often write xy instead of $x \cdot y$.

Remark. We say that "S is closed under the operation $\cdot$", when we want to emphasize that for any $x, y \in S$ the result of the operation, xy, is an element of S. However note that closure is really part of the definition of a binary operation on a set, and it is implicitly assumed whenever we consider such an operation.

Definition 1.2. A *group* is a pair $(G, \cdot)$ where G is a set and $\cdot$ is a binary operation on G called *group multiplication*, satisfying the following properties:

1. (*associativity*) for all $x, y, z \in G$ we have $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
2. (*identity element*) there exists $e \in G$ such that $e \cdot x = x \cdot e = x$ for all $x \in G$
3. (*inverses*) for each $x \in G$, there is an element $y \in G$ such that $xy = e = yx$.

Remark. Although a group is a pair, we will usually refer to the group by only naming the underlying set, G.

Proposition 1.3. *In a group G, the element e satisfying the second axiom of Definition 1.2 is unique, and we thus refer to it as the* identity element *of G.*

Proof. If $ex = x = xe$ and $e'x = x = xe'$ for all x, then $e = ee' = e'$. □

Proposition 1.4. *In a group G, for each x, the element y satisfying the last axiom of Definition 1.2 is unique.*

Proof. For a given x, if $yx = xy = e$ and $zx = xz = e$ fo some y and z, then $z = ez = (yx)z = y(xz) = ye = y$. □

Remark. We will call the element y satisfying the last axiom of Definition 1.2 *the inverse* of x and we will henceforth denote it by x^{-1}.

Lemma 1.5 (Properties of groups)**.** *If G is a group and $x, y, z, a_1, \ldots, a_n \in G$, then:*

1. *if $xy = xz$, then $y = z$.*
2. *if $yx = zx$, then $y = z$.*
3. *$(x^{-1})^{-1} = x$.*
4. *$(a_1 \ldots a_n)^{-1} = a_n^{-1} \ldots a_1^{-1}$.*
5. *$(x^{-1}yx)^n = x^{-1}y^n x$.*

Proof. Exercise. □

Definition 1.6. A group G is an *abelian group* if $\cdot$ is commutative; i.e., $x \cdot y = y \cdot x$ for all $x, y \in G$. Often, but not always, the group operation for an abelian group is written as $+$ instead of $\cdot$. In this case the inverse of an element x is written $-x$.

Example.

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ and $(\mathbb{C}, +)$ are abelian groups.
- For any n, let $\mathbb{Z}/n$ denote the integers modulo n. Then $(\mathbb{Z}/n, +)$ is an abelian group where $+$ denotes addition modulo n.
- For any field F (e.g., $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{Z}/p$ for a prime p), the set $F^\times := F \setminus \{0\}$ is an abelian group under the usual multiplication.

Example. For any set S, the permutations on S

$$\mathrm{Perm(S)} = \{\mathrm{f} : \mathrm{S} \to \mathrm{S} \mid \mathrm{f \text{ is a bijection}}\}$$

form a group under composition.

Example. For any field F and positive integer n, let

$$\mathrm{GL}_n(F) = \{\text{invertible } n \times n \text{ matrices with entries in } F\}.$$

By invertible I mean those matrices that have two-sided inverses, but in turns out that if an $n \times n$ matrix has a left inverse then it it is automatically a right inverse too, and vice versa. Then $\mathrm{GL}_n(F)$ is a group under matrix multiplication.

Note that $GL_1(F)$ is the same thing as $(F^\times, \cdot)$.

Exercise. These example are infinite if F is infinite, but if we take $F = \mathbb{Z}/p$ for a prime p, then $\mathrm{GL}_n(\mathbb{Z}/p)$ is a finite group. Can you find its cardinality?

Exercise. Give an example of a pair $(G, \cdot)$ that satisfies axioms 1 and 2 of Definition 1.2 and an element of G that has a *left* inverse but not a *right* inverse.

We now discuss the impotant example of dihedral groups in detail.

1.1.1 Dihedral groups

For any integer $n \geq 3$, let P_n denote a regular n-gon. The *dihedral group* D_{2n} is the group of symmetries of P_n. Let us make this more precise:

An *isometry* of the plane is a function $f : \mathbb{R}^2 \to \mathbb{R}^2$ that is a bijection and preserves the Euclideal distance ($d(f(A), f(B)) = d(A, B)$ for any $A, B \in \mathbb{R}^2$). A *symmetry* of P_n is an isometry that maps P_n to itself. By the latter I don't mean that f fixes each of the points of P_n, but rather that $f(P_n) = P_n$, that is every point of P_n is mapped to a (possibly different) point of P_n and every point of P_n is the image of some point in P_n via f. It is clear that the composition of two symmetries of P_n is again a symmetry of P_n, so that composition is a binary operation on D_n.

We give the formal definition:

Definition 1.7. The *dihedral group* D_{2n} is the set of symmetries of the regular n-gon P_n equipped with the binary operation given by composition.

Justification: Associativity of composition is a general property of functions (inherited from $\text{Perm}(\mathbb{R}^2)$). It is easy to see that its the inverse function of an isometry is also an isometry. Using this, it is clear that every element of D_{2n} has an inverse. The identity function on $\mathbb{R}^2$ belongs to D_{2n} and is the identity element.

Remark. We will see very soon that the index $2n$ in D_{2n} corresponds to the number of elements of this group (symmetries of P_n).

Assume that the regular n-gon P_n is drawn in the plane with its center at the origin and one vertex on the x axis. If r denotes rotation about the origin by $\frac{2\pi}{n}$ radians counter-clockwise, then $r \in D_{2n}$. It's inverse is rotation by $2\pi/n$ clock-wise. For another example, for any line of symmetry of P_n, reflection about that line gives an element of D_{2n}. By our convention for how to draw P_n, the x-axis is a line of symmetry for P_n, and we let s denote reflection about the x-axis.

It is clear that $r^n = e$ and $s^2 = e$; the latter gives that $s^{-1} = s$ (by multiplying both sides by s^{-1}). Slightly less clear is the important relation $srs^{-1} = r^{-1}$, which may equivalently be written as $srs = r^{-1}$ or $srsr = e$.

August 22, 2018

Proposition 1.8. *Every element in D_{2n} can be written as r^j or $r^j s$ for $0 \leq j \leq n-1$. Moreover, no two of these expressions are the same element, and thus D_{2n} has exactly $2n$ elements.*

Proof. We will use some geometric notions freely without complete justification. For example, we use that if an isometry of $\mathbb{R}^2$ fixes two points A and B, then it is either the identity element or it is reflection about the line AB. We also use that every element of D_{2n} maps the origin to itself (since the origin is the center of mass of P_n). Finally, we use that every isometry of $\mathbb{R}^2$ is either *orientation preserving* or *orientation reversing*.

Label the vertices of P_n as $V_0, \ldots, V_{n-1}$, with V_0 being the vertex located on the positive s-axis, V_1 being the vertex adjacent to V_0 in the counter-clockwise direction, etc. We have $r(V_0) = V_1$, $r(V_1) = V_2$, etc., and so $r^j(V_0) = V_{j \pmod n}$.

Let α be an arbitrary symmetry of P_n. Then $\alpha(V_0) = V_j$ for some $0 \leq j \leq n-1$. Then the element $r^{-j}\alpha$ fixes V_0 and the origin, and hence either $r^{-j}\alpha = e$ or $r^{-j}\alpha = s$ from the discussion above. We get that $\alpha = r^j$ or $\alpha = r^j s$, proving the first assertion.

Since $r^j(V_0) = V_{j \pmod n}$, we see that if $r^j = r^i$ for $0 \leq i, j \leq n-1$, then $i = j$. We have $r^j s \neq r^i$ for any i, j since the former is orientation reversing and the latter is orientation preserving. If $r^i s = r^j s$ for $0 \leq i, j \leq n-1$, then upon multiplying on the left of s^{-1} we get $i = j$. □

This seems like a good time to introduce at an intuitive level the notion of a *presentation of a group*. We will make it precise eventually, but the idea is to give generators and relations that completely determine a group. For example, we will show that a presentation of D_{2n} is

$$D_{2n} = \langle r, s \mid r^n = 1, s^2 = 1, srs^{-1} = r^{-1} \rangle.$$

Definition 1.9.

- A *presentation* for a group is a way to specify a group in the following format

$$G = \langle \text{ set of generators } \mid \text{ set of relations } \rangle.$$

- A set S is said to *generate* or be a *set of generators* for a group if every element of the group can be expressed in some as a product of the elements of S and their inverses (with repetitions allowed).

- A *relation* is an identity satisfied by some expressions involving the generators and their inverses. We usually record just enough relations so that every valid equation involving the generators is a consequence of those listed here and the axioms of a group.

To illustrate this, let us prove that the group described abstractly by the presentation $X_{2n} = \langle r, s \mid r^n = 1, s^2 = 1, srs^{-1} = r^{-1} \rangle$ is the same as D_{2n}. Here $1 = 1_{\mathbb{R}^2}$ is the identity map on $\mathbb{R}^2$.

Proposition 1.10. *Let $r : \mathbb{R}^2 \to \mathbb{R}^2$ denote counterclockwise rotation around the origin by $\frac{2\pi}{n}$ radians and let $s : \mathbb{R}^2 \to \mathbb{R}^2$ denote reflection about the x-axis respectively. Set $X_{2n} = \langle r, s \mid r^n = 1, s^2 = 1, srs^{-1} = r^{-1} \rangle$. Then $D_{2n} = X_{2n}$, that is*

$$D_{2n} = \langle r, s \mid r^n = 1, s^2 = 1, srs^{-1} = r^{-1} \rangle.$$

Proof. Proposition 1.8 gives that $\{r, s\}$ is a set of generators for D_{2n} and we also know that the relations listed above $r^n = 1, s^2 = 1, srs^{-1} = r^{-1}$ are true. The concern is that we may not have discovered all the relations of D_{2n} (or rather, enough relations so that any other valid relation follows as a consequence of the ones listed).

Assume that D_{2n} has more relations than X_{2n} does. Then D_{2n} would be a group of cardinality strictly smaller than that of X_{2n}, i.e. $|D_{2n}| < |X_{2n}|$. (This will become more clear once we properly define presentations). We show below that in fact $|X_{2n}| \leq 2n = |D_{2n}|$, thus obtaining a contradiction.

Now we show that X_{2n} has at most $2n$ elements using just the information contained in the presentation: Every element $x \in X_{2n}$ can be written as

$$x = r^{m_1} s^{n_1} r^{m_2} s^{n_2} \cdots r^{m_j} s^{n_j}$$

for some j and integers (possibly negative) $m_1, \ldots, m_j, n_1, \ldots, m_j$. (Note that, e.g., m_1 could be 0 so that expressions beginning with a power of s are included in this list.) As a consequence of the last relation, we have

$$sr = r^{-1}s,$$

and its not hard to see that this implies

$$sr^m = r^{-m}s$$

for all m. Thus, we can "slide an s past a power of r", at the cost of changing the sign of the power. Doing this repeatedly gives that we can rewrite x as

$$x = r^M s^N$$

By the first relation, $r^n = 1$, from which it follows that $r^a = r^b$ if a and b are congruent modulo n. Thus we may assume $0 \leq M \leq n-1$. Likewise, we may assume $0 \leq N \leq 1$. This gives a total of at most $2n$ elements. □

Note that we have *not* shown $X_{2n} = \langle r, s \mid r^n, s^2, srs^{-1} = r^{-1} \rangle$ has at least $2n$ elements, using just the presentation. But for this particular example, since we know the group presented is the same as D_{2n}, we know from Proposition 1.8 that it has exactly $2n$ elements.

In general, given a presentation, it is very difficult to prove certain expressions are not actually equal to each other. In fact,

> There is no algorithm that, given any group presentation as an input, can decide whether the group is actually the trivial group with just one element.

and perhaps more strikingly

> There exist a presentation with finitely many generators and finitely many relations such that whether or not the group is actually the trivial group with just one element is *independent of the standard axioms of mathematics*!

1.1.2 Symmetric groups

Let's introduce another very important example: symmetric groups.

Definition 1.11. For any set X, the permutation group on X is the set $\mathrm{Perm}(X)$ of all bijective (one-to-one and onto) functions from X to itself equipped with the composition of functions as its binary operation.

Notation. For an integer $n \geq 1$, define $[n] = \{1, \ldots, n\}$ and let $S_n = \mathrm{Perm}([n])$. An element of S_n is called a *permutation on n symbols*.

We can write an element σ of S_n as a table of values:

1	2	3	$\cdots$	n
$\sigma(1)$	$\sigma(2)$	$\sigma(3)$	$\cdots$	$\sigma(n)$

Remark 1.12. S_n has $n!$ elements since there are n choices for $\sigma(1)$, $n-1$ choices for $\sigma(2)$ once $s(1)$ has been chosen, ... down to 1 choice for $s(n)$ once the other values have been chosen.

It is customary to use *cycle notation* for permutations.

Definition 1.13. If $i_1, \ldots, i_m$ are distinct integers between 1 and n, then $\sigma = (i_1\, i_2\, \ldots i_m)$ denotes the element of S_n that satisfies $\sigma(i_1) = i_2$, $\sigma(i_2) = i_3, \ldots$, $\sigma(i_{m-1}) = i_m$ and $\sigma(i_m) = i_1$, and which fixes all elements of $[n] \setminus \{i_1, \ldots, i_m\}$. Such a permutation is called a *cycle* or an *m-cycle* when we want to emphasize its length.

Any 1-cycle is the identity function. A 2-cycle is often called a *transposition*.

Note that distinct lists of integers represent the same cycle if they are cyclical rearrangements of each other, e.g., $(1\,2\,3) = (2\,3\,1)$.

Exercise 1.14. Disjoint cycles commute, that is, if $i_1, i_2 \ldots i_m, j_1, j_2 \ldots j_k \in [n]$,

$$\sigma_1 = (i_1\, i_2\, \ldots i_m), \quad \sigma_2 = (j_1\, j_2\, \ldots j_k)$$

and

$$\{i_1, i_2, \ldots i_m\} \cap \{j_1, j_2, \ldots j_k\} = \emptyset$$

then $\sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1$.

August 24, 2018

Proposition 1.15. *For $\sigma \in S_n$, σ can be written as a product (composition) of disjoint cycles, and such a factorization is unique up to the ordering of the factors.*

Proof. (informal sketch) We will give a formal proof of this proposition later, but for now we record that the main idea is to look at the orbits of the permutation σ, meaning the subsets of $[n]$ that have the form

$$O_i = \{i, \sigma(i), \sigma^2(i), s^3(i), \ldots\}$$

and turn them into cycles $\tau_i = (i\,\sigma(i)\,\sigma^2(i)\,\sigma^3(i)\,\ldots\,\sigma^{n_i-1}(i))$, where n_i is the smallest positive integer such that $\sigma^{n_i}(i) = i$. Then, letting S be a set of indices for the distinct τ_i, a factorization of σ will be

$$\sigma = \prod_{i \in S} \tau_i.$$

□

Remark 1.16. For the uniqueness part of the above proposition one needs to establish a convention regarding 1-cycles, that is one needs to stipulate either that the 1-cycles will not be recorded (which gives the shortest such factorization) or that all the 1-cycles will be recorded (which gives the longest such factorization, but also the only one that makes it clear what the number n is).

Definition 1.17. For $\sigma \in S_n$, the *cycle type* of σ is the unordered list of lengths of cycles that occur in the unique decomposition of σ into a product of disjoint cycles.

For example the element

$$(3\,4)(1\,5)(2\,6\,7)(9\,8\,11)(15\,16\,17\,105\,114)$$

of S_{156} has cycle type $2, 2, 3, 3, 5$. (Note that the n of S_n is not recorded, but is implicit.)

Corollary 1.18. *Every permutation is a product of transpositions; i.e., S_n is generated by transpositions.*

Proof. By Proposition 1.15, it suffices to prove this for a single cycle because we first decompose the permutation as a product of cycles and then we decompose each cycle as a product of transpositions. For a cycle $(i_1\,i_2\,\cdots\,i_p)$ the identity

$$(i_1\,i_2\,\cdots\,i_p) = (i_1\,i_2)(i_2\,i_3)\cdots(i_{p-2}\,i_{p-1})(i_{p-1}\,i_p)$$

is seen to hold by direct calculation. □

1.1.3 The quaternions

For our last example we mention the group of *quaternions*, written Q_8.

Definition 1.19. The quaternion group Q_8 is a group with 8 elements

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

satisfying the following relations: 1 is the identity element and

$$i^2 = -1, j^2 = -1, k^2 = -1, ij = k, jk = i, ki = j,$$

$$(-1)i = -i, (-1)j = -j, (-1)k = -k, (-1)(-1) = 1.$$

To verify that this really is a group is rather tedious, since the associative property takes forever to check. Here is a better way: In the group $\mathrm{GL}_2(\mathbb{C})$, define elements

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, A = \begin{bmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{bmatrix}, B = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, C = \begin{bmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{bmatrix}$$

where I have written $\sqrt{-1}$ for the complex number whose square is -1 to avoid confusion with the symbol $i \in Q_8$. Let $-I, -A, -B, -C$ be the negatives of these matrices.

Then we can define an injective map $f : Q_8 \to \mathrm{GL}_2(\mathbb{C})$ by assigning

$$\begin{aligned} 1 &\mapsto I, & -1 &\mapsto -I \\ i &\mapsto A, & -i &\mapsto -A \\ j &\mapsto B, & -j &\mapsto -B \\ k &\mapsto C, & -k &\mapsto -C. \end{aligned}$$

It can be checked directly that this map has the nice property (called being a *group homomorphism*) that

$$f(xy) = f(x)f(y) \text{ for any elements } x, y \in \mathbb{Q}_8.$$

Let us now prove associativity for Q_8 using this information:

Claim: For any $x, y, z \in Q_8$, we have $(xy)z = x(yz)$.

Proof. By using the property $f(xy) = f(x)f(y)$ as well as associativity of multiplication in $\mathrm{GL}_2(\mathbb{C})$ (marked by $*$) we obtain

$$f((xy)z) = f(xy)f(z) = (f(x)f(y))\, f(z) \overset{*}{=} f(x)\,(f(y)f(z)) = f(x)f(yz) = f(x(yz)).$$

Since f is injective and $f((xy)z) = f(x(yz))$, we deduce $(xy)z = x(yz)$. □

The subset $\{\pm I, \pm A, \pm B, \pm C\}$ of $\mathrm{GL}_2(\mathbb{C})$ is a *subgroup* (a term we define carefully later), meaning that it is closed under multiplication and taking inverses. (For example, $AB = C$ and $C^{-1} = -C$.) This proves it really is a group and one can check it satisfies an analogous list of identities as the one satisfied by Q_8.

1.2 Homomorphisms and isomorphisms

Definition 1.20. If G and H are groups, a *homomorphism* from G is H is a function $f : G \to H$ such that $f(x \cdot_G y) = f(x) \cdot_H f(y)$, where $\cdot_G$ and $\cdot_H$ denote the multiplication rules for G and H, respectively.

Definition 1.21. A homomorphism $f : G \to H$ is called an *isomorphism* if there exists a homomorphism $g : H \to G$ such that $f \circ g = \mathrm{id}_H$ and $g \circ f = \mathrm{id}_G$.

If $f : G \to H$ is an isomorphism, G and H are called *isomorphic*, written $G \cong H$.

Example.

- The identity map is a group isomomorphism for any group G.
- The exponential map $\exp : (\mathbb{R}, +) \to (\mathbb{R} \setminus \{0\}, \cdot)$ is a homomorphism. So is $\ln : (\mathbb{R}_{>0}, \cdot) \to (\mathbb{R}, +)$. In fact, these maps are inverse to each other so we obtain an isomorphism . $(\mathbb{R}, +) \cong (\mathbb{R}_{>0}, \cdot)$.
- For any positive integer n and field F, the map determinant map $\det : \mathrm{GL}_n(F) \to (F \setminus \{0\}, \cdot)$ is a group homomorphism.

August 27, 2018

Lemma 1.22 (Properties of homomorphisms)**.** *If $f : G \to H$ is a homomorphism of groups, then*

1. *$f(e_G) = e_H$ and*
2. *$f(x^{-1}) = f(x)^{-1}$.*

Proof. For the first, $f(e_G) = f(e_G e_G) = f(e_G)f(e_G)$ and now multiply by $f(e_G)^{-1}$. For the second, $f(x^{-1})f(x) = f(e) = e$ implies $f(x^{-1}) = f(x)^{-1}$. □

Definition 1.23. The *kernel* of a group homomorphism $f : G \to G$ is

$$\mathrm{Ker}(f) = \{g \in G \mid f(g) = e_H\}.$$

Proposition 1.24. *A group homomorphism $f : G \to H$ is one-to-one if and only if* $\mathrm{Ker}(f) = \{e_G\}$.

Proof. $\Rightarrow$ is immediate from the definitions (since $e_G \in \mathrm{Ker}(f)$ for all homomorphisms f). If $\mathrm{Ker}(f) = \{e_G\}$ and $f(h) = f(h')$ then $f(h^{-1}h') = f(h)^{-1}f(h') = e_H$ and thus $h^{-1}h' = e_G$ which implies $h = h'$. □

Remark 1.25. I have defined the notion of isomorphism in Definition 1.21 differently than given in the textbook. The reason is that the correct meaning of the word "isomorphism" in any context (sets, groups, rings, fields, topological spaces, whatever) is always "a morphism that has a two-sided inverse". In many contexts, such as sets, groups, rings and fields this turns out to be equivalent to the notion of being "one-to-one and onto". But there are contexts in which this is not the case. For example a one-to-one and onto continuous map of topological spaces need not be a homeomorhism. (A homeomorphism is term one uses for isomorhism of topological spaces, for historical reasons.)

Proposition 1.26. *Suppose $f : G \to H$ is a group homomorphism. Then f an isomorphism if and only if f is bijective (one-to-one and onto).*

Proof. The $\Rightarrow$ direction follows by recalling that a function $f : X \to Y$ between two sets is bijective if and only if there is a function $g : Y \to X$ such that $f \circ g = \mathrm{id}_Y$ and $g \circ f = \mathrm{id}_X$.

For the $\Leftarrow$ direction, if f is bijective homomorphism, then it certainly has a *set-theoretic* two-sided inverse g. But we need to show g is actually a homomorphism: for $x, y \in H$ we have $f(g(xy)) = xy = f(g(x))f(g(y)) = f(g(x)g(y))$. Since f is one-to-one, $g(xy) = g(x)g(y)$. □

From the above proposition we deduce

Definition (Alternate definition for group isomorphism)**.** A function $f : G \to H$ between two groups is an isomorphism if and only if f is a bijective homomorphism.

Let us define a few more notions:

Definition 1.27. In a group G, the *order of an element* x is the least positive integer n such that $x^n = e$. If no such n exists, we say x has infinite order. We write $|x|$ for the order of x.

Definition 1.28. The *order of a group* G is the cardinality of the set G, denoted $|G|$.

Definition 1.29. An *isomorphism invariant* is a property P such that whenever $G \cong H$ and G has P then H has P.

Theorem 1.30. *The following are isomorphism invariants:*

1. *the order of the group,*
2. *the set of orders of elements in the group,*
3. *being abelian,*
4. *the order of the center of the group,*
5. *being finitely generated,*

Proof. Let G and H be isomporphic groups with $f : G \to H$ a group isomorphism.

1. Since f is a bijection by Proposition 1.26, and two sets have the same cardinality if and only if they are in bijective correspondence to each other, we obtain that $|G| = |H|$.
2. We wish to show $\{|x| \mid x \in G\} = \{|y| \mid y \in H\}$.

   " $\subseteq$ " follows by problem 2(c) of homework 1, since $x \in G$ yields $f(x) \in H$ and $|f(x)| = |x|$.

   " $\supseteq$ " also follows by problem 2(c) of homework 1, applied to the group isomorphism f^{-1}, since $y \in G$ yields $f^{-1}(y) \in G$ and $|f^{-1}(y)| = |y|$.

3. If $y_1, y_2 \in H$ then there exist $x_1, x_2 \in G$ such that $f(x_i) = y_i$. Then we have

$$y_1 y_2 = f(x_1)f(x_2) = f(x_1 x_2) \overset{*}{=} f(x_2 x_1) = f(x_2)f(x_1) = y_2 y_1,$$

where $*$ indicates the usage of the abelian property for G.

4. Exercise. The idea is to show f induces an isomorphism $Z(G) \cong Z(H)$.

5. Exercise. Show that if S generates G then $f(S) = \{f(s) \mid s \in S\}$ generates H.

□

Proposition 1.31. *If P is an isomorphism invariant, G is a group that has P, and H is a group that does not have P, then G is not isomorphic to H.*

Proof. This statement is the contrapositive of Definition 1.29. □

Example.

- $S_n \cong S_m$ if and only if $n = m$ by comparing the orders of the groups.
- $\mathbb{Z}/6 \ncong S_3$ because $\mathbb{Z}/6$ is abelian and S_3 is not abelian.
- $D_{24} \ncong S_4$ because $|Z(D_{24})| = 2$ by HW 1 and $|Z(S_n)| = 1$ (i.e., $Z(S_n) = \{\mathrm{id}_{[n]}\}$).

August 29, 2018

1.3 Group actions

We come to one of the central concepts in group theory, that of an action of a group on a set.

Definition 1.32. For a group $(G, \cdot)$ and set S, an *action* of G on S is a function

$$G \times S \to S,$$

typically written as $(g, s) \mapsto g \cdot s$, such that

1. $g \cdot (g' \cdot s) = (gg') \cdot s$ for all $g, g' \in G$ and $s \in S$.
2. $e_G \cdot s = s$ for all $s \in S$.

Remark 1.33. To make the first axiom clearer, throughout this section we will write $\cdot$ for the action of G on S and no symbol (concatenation) for the multiplication of two elements in the group G.

A group action is the same thing as a group homomorphism.

Proposition 1.34 (Permutation representation)**.** *Assume $(G, \cdot)$ is a group and S is a set.*

1. *If $\cdot$ is an action of G on S, then the function $\rho : G \to \mathrm{Perm}(S)$ defined as $\rho(g) = \sigma_g$, where $\sigma_g : S \to S$ is the function given by $\sigma_g(s) = g \cdot s$, is a well defined homomorphism of groups.*

2. *Conversely, if $\rho : G \to \mathrm{Perm}(S)$ is a group homomorphism, the rule $g \cdot s := \rho(g)(s)$ defines an action of G on S.*

Proof. Assume we are given an action $\cdot$ of G on S. We need to check that for all g, σ_g really is a permutation of S. We'll show this by proving that σ_g has a two-sided inverse and that inverse is $\sigma_{g^{-1}}$.

We have

$$\begin{aligned}
(\sigma_g \circ \sigma_{g^{-1}})(s) &= \sigma_g(\sigma_{g^{-1}}(s)) && \text{(def of composition)} \\
&= g \cdot (g^{-1} \cdot s) && \text{(def for } \sigma_g \text{ and } \sigma_{g^{-1}}\text{)} \\
&= (gg^{-1}) \cdot s && \text{(first property of a group action)} \\
&= e_G \cdot s && \text{(group axiom)} \\
&= s && \text{(second property of a group action)}
\end{aligned}$$

thus $\sigma_g \circ \sigma_{g^{-1}} = \mathrm{id}_S$ and a similar argument shows that $\sigma_{g^{-1}} \circ \sigma_g = \mathrm{id}_S$

Finally, we wish to show $\rho(gg') = \rho(g) \circ \rho(g')$, equivalently $\sigma_{gg'} = \sigma_g \circ \sigma_{g'}$. Since

$$\sigma_{gg'}(s) = (gg') \cdot s = g \cdot (g' \cdots) = \sigma_g\left(\sigma_{g'}(s)\right) = (\sigma_g \circ \sigma_{g'})(s),$$

holds for all s, this proves ρ is a homomorphism.

Given a homomorphism ρ, the function $G \times S \to S$ defined as $g \cdot s = \rho(g)(s)$ is an action because $g'(gs) = \rho(g')(\rho(g)(s)) = (\rho(g') \circ \rho(g))(s) = \rho(gg')(s) = (gg')s$, and $e_G s = \rho(e_G)(s) = \mathrm{id}(s) = s$. □

Example (Trivial action)**.** For any group G and any set S, $g \cdot s := s$ defines an action, the *trivial action*. The associated group homomorphism is $G \to \mathrm{Perm}(S)$ by $g \mapsto \mathrm{id}_S$.

Example. The group D_{2n} acts on the vertices of P_n, which I will number as $1, \ldots, V_n$ in a counterclockwise fashion, with V_1 on the positive x-axis. That is, D_{2n} acts on $\{V_1, \ldots, V_n\}$. In detail, for $g \in D_{2n}$ and a number $1 \leq j \leq n$, set $g \cdot V_j = V_i$ if and only if $g(V_j) = V_i$. This satisfies the two axioms of a group action.

Let $\rho : D_{2n} \to \mathrm{Perm}\left(\{V_1, \ldots, V_n\}\right) \cong S_n$ be the associated group homomorphism. In this particular example, ρ is injective, because if an element of D_{2n} fixes all n vertices of a polygon, then it must be the identity map. More generally, if an isometry of $\mathbb{R}^2$ fixes any three non-colinear points, then it is the identiy. To see this, note that given three non-colinear points, every point in the plane is uniquely determined by its distance from these three points. (Think about a circle centered at each point, and where they can meet.)

Definition 1.35. An action of a group G on a set S is called *faithful* if the associated group homomorphism is one-on-one. Equivalently, an action is faithful if and only if for a given $g \in G$, whenever $g \cdot s = s$ for all $s \in S$, it must be that $g = e_G$.

For example, the action of D_{2n} on the n vertices of P_n is faithful, but the trivial action of a group is not faithful.

Example (A group acts on itself by left multiplication = *left regular action*)**.** Let G be any group and define an action $\cdot$ of G on G (regarded as just a set) by the rule

$$g \cdot x = gx, \text{ for } g \in G \text{ and } x \in G.$$

This is an action since multiplication is associative and $e_G \cdot x = x$ for all x.

The left regular action of G on itself **is faithful**, since if $g \cdot x = x$ for all x (or even for just one x then $g = e$. It follows that the associated homomorphism

$$\rho : G \to \text{Perm}(G)$$

is injective, where on the right we mean the set of bijective functions from G to itself.

August 31, 2018

Example (A group acts on itself by conjugation = conjugation action)**.** Let G be any group and fix an element $g \in G$. Define *the conjugation action* of G on itself by setting

$$g \cdot x = gxg^{-1} \text{ for any } g, x \in G.$$

The action of G on itself by conjugation **is not necessarily faithful**. In fact the kernel of the permutation representation for the conjugation action is the center $Z(G)$. In detail, if $\rho : G \to \text{Perm}(G)$ is the permutation representation for G acting on G by conjugation, then

$$\begin{aligned} g \in \text{Ker}\,\rho &\iff g \cdot x = x, \forall x \in G \iff gxg^{-1} = x, \forall x \in G \\ &\iff gx = xg, \forall x \in G \iff g \in Z(G). \end{aligned}$$

Definition 1.36. Let G be a group acting on a set S. The *equivalence relation* on S induced by the action of G, written $\sim_G$, is defined by $s \sim_G s'$ if and only if there is a $g \in G$ such that $s' = g \cdot s$. The equivalence classes of $\sim_G$ are called *orbits*, specifically the equivalence class

$$\text{Orbit}_G(s) = \{g \cdot s \mid g \in G\}$$

is the orbit of S. The set of equivalence classes with respect to $\sim_G$ is written S/G.

Lemma 1.37. *: Let G be a group acting on a set S. Then*

1. *$\sim_G$ is an equivalence relation*
2. *for any $s, s' \in S$ either $\text{Orbit}_G(s) = \text{Orbit}_G(s')$ or $\text{Orbit}_G(s) \cap \text{Orbit}_G(s') = \emptyset$*
3. *$S = \bigcup_{\text{Orbit}_G(s) \in X/G} \text{Orbit}_G(s)$*

Proof. Part 1. is a problem on HW 2. Parts 2. and 3. are properties of the equivalence classes of any equivalence relation. □

Remark. The last two properties say that the orbits of the G action partition S.

1.4 Subgroups

1.4.1 Definition and examples

Definition 1.38. A nonempty subset H of a group G is called a *subgroup* provided H is a group under the multiplication law of G. The fact that H is a subgroup of G is denoted $H \leq G$ or $H < G$ if we also mean that $H \neq G$.

Example. $\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$ and $\mathbb{Z}^\times < \mathbb{Q}^\times < \mathbb{R}^\times < \mathbb{C}^\times$.

Lemma 1.39 (Subgroup tests)**.**

[Two-step test] If a subset H of a group G is nonempty and closed under multiplication and inversion, then H is a subgroup.

[One-step test] If a subset H of a group G is nonempty and satisfies for all $x, y \in H$, $xy^{-1} \in H$, then H is a subgroup.

Proof. 2. We prove the one-step test first.

Assume H is non-empty and for all $x, y \in H$, $xy^{-1} \in H$. Since H is non-empty, there is an $h \in H$ and hence $e_G = hh^{-1} \in H$. Since $e_G x = x = xe_G$ for any $x \in H$, e_G is an identity element for H. For any $h \in H$, $h^{-1} = eh^{-1} \in H$, and so every element of H has an inverse inside H. For $x, y \in H$ we have $y^{-1} \in H$ and thus $xy = x(y^{-1})^{-1} \in H$ and hence H is closed under $\cdot$. This means that the restriction of the group operation of G to H is a well-defined group operation. This operation is associative by the axioms for the group G. The axioms of a group have now been established for $(H, \cdot)$.

1. We prove the two-step test.

Assume H is non-empty and closed under multiplication and inversion. Then, for $x, y \in H$ we have $y^{-1} \in H$ and $xy^{-1} \in H$. Since the hypothesis of the one-step test is satisfied, H is a subgroup of G. □

Proposition 1.40 (Examples of subgroups)**.**

1. *$\{e_G\}$ and G are the trivial subgroups of G.*
2. *If H is a subgroup of G and K is a subgroup of H, then K is a subgroup of G.*
3. *If H_α is a subgroup of G for all α in an index set J, then $H = \bigcap_{\alpha \in J} H_\alpha$ is a subgroup of G.*
4. *If $f : G \to H$ is a homomorhism of groups, then the set-theoretic image of f,*

$$\mathrm{Im}(f) := \{f(g) \mid g \in G\}$$

is a subgroup of H.

5. *If $f : G \to H$ is a homomorphism of groups, then the kernel of f,*

$$\mathrm{Ker}(f) := \{g \in G \mid f(g) = e_H\},$$

is a subgroup of G.

Proof. 1. Exercise.

2. H is not empty since $e_G \in H_\alpha$ for all $\alpha \in J$. If $x, y \in G$, then for each α, $x, y \in H_\alpha$ and hence $xy^{-1} \in H_\alpha$. It follows that $xy^{-1} \in H$.

3. To see this, note that $\mathrm{Im}(f) \neq \emptyset$ since G is non-empty. If $x, y \in \mathrm{Im}(f)$, then $x = f(a)$ and $y = f(b)$ for some $a, b \in G$ and hence $xy^{-1} = f(a)f(b)^{-1} = f(ab^{-1}) \in \mathrm{Im}(f)$.

4. To see this, using the one-step subgroup test note that if $f(x) = f(y) = e_G$ then $f(xy^{-1}) = f(x)f(y)^{-1} = e_G$. So, if $x, y \in \mathrm{Ker}(f)$ then $xy^{-1} \in \mathrm{Ker}(f)$.

5. The center $Z(G)$ is the kernel of the permutation representation $G \to \mathrm{Perm}(G)$ for the conjugation action, so by part 4. $Z(G)$ is a subgroup of G. □

Example. For any field F, the *special linear group*

$$\mathrm{SL}_n(F) = \{A \mid A = n \times n \text{ matrix with entries in } F, \det(A) = 1_F\}$$

is a subgroup of the general linear group $\mathrm{GL}_n(F)$ because $\mathrm{SL}_n(F)$ is the kernel of the group homomorphism $\det : \mathrm{GL}_n(F) \to F^\times$.

September 5, 2018

Definition 1.41. Given a group G and a subset X of G, the *subgroup of G generated by X* is

$$\langle X \rangle := \bigcap_{H \leq G, H \supseteq X} H.$$

If $X = \{x\}$ is a set with one element then we write $\langle X \rangle = \langle x \rangle$ and we refer to this as the *cyclic subgroup generated by x*.

By part 2 of Proposition 1.40, $\langle X \rangle$ really is a subgroup of G. By definition, the subgroup generated by X it is the smallest (with respect to containment) subgroup of G that contains X, meaning that $\langle X \rangle$ is contained in any subgroup that contains X.

Lemma 1.42. *For a subset X of G, the elements of $\langle X \rangle$ can be described as:*

$$\langle X \rangle = \left\{ x_1^{j_1} \cdots x_m^{j_m} \mid m \geq 0, j_1, \ldots, j_m \in \mathbb{Z} \text{ and } x_1, \ldots, x_m \in X \right\}.$$

Proof. Let $S = \left\{ x_1^{j_1} \cdots x_m^{j_m} \mid m \geq 0, j_1, \ldots, j_m \in \mathbb{Z} \text{ and } x_1, \ldots, x_m \in X \right\}$. Since $\langle X \rangle$ is a subgroup that contains X, it is closed under products and inverses, and thus must contain all elements of S.

For the opposite containment, we just need to show the set S really is a subgroup. We use the one step test:

- $S \neq \emptyset$ since we allow $m = 0$ and declare the empty product to be e_G.
- If $x_1^{j_1} \cdots x_m^{j_m}$ and $y_1^{i_1} \cdots y_n^{i_m}$ are in S then

  $$x_1^{j_1} \cdots x_m^{j_m} (y_1^{i_1} \cdots y_n^{i_m})^{-1} = x_1^{j_1} \cdots x_m^{j_m} y_n^{-i_m} \cdots y_1^{-i_1}$$

  is also in S.

Therefore $S \leq G$ and $X \subseteq S$ (by taking $m = 1$ and $j_1 = 1$) and by the minimality of $\langle X \rangle$ we obtain $\langle X \rangle \subseteq S$. □

Example. The Lemma implies that for an element x of a group G, $\langle x \rangle = \{x^j \mid j \in \mathbb{Z}\}$.

Example. $D_{2n} = \langle r, s \rangle$, meaning that D_{2n} is the subgroup of D_{2n} generated by $\{r, s\}$. Do not mistake this for a presentation with no relations.

Example. For any n, S_n is generated by the collection of "adjacent transpositions".

Interaction of subgroups with isomorphism invariants

We record some important facts about the relationship between finite groups and their subgroups.

Order of the group:

- Every subgroup of a finite group is finite.
- There exist infinite groups with finite subgroups.
- **Theorem 1.43** (Lagrange's Theorem)**.** *If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.*

  Proof. See HW 2. □

Orders of elements:

- If $H \subseteq G$, then the set of orders of elements of H is a subset of the set of orders of elements of G.

Abelian:

- Every subgroup of an abelian group is abelian.
- There exist nonabelian groups with abelian subgroups.
- Every cyclic subgroup is abelian.

Finitely generated:

- There exist a finitely generated group G and a subgroup H of G such that H is not finitely generated.

1.4.2 Cyclic groups

Definition 1.44. If G is a generated by a single element, i.e. $G = \langle x \rangle$ for some $x \in G$, then G is called a *cyclic group*.

Remark 1.45. The same cyclic group may have different generators, for example

$$\langle x \rangle = \langle x^{-1} \rangle.$$

Definition 1.46. In a group G, the *order* of an element x is the least positive integer n such that $x^n = e$. If no such n exists, we say x has infinite order. We write $|x|$ for the order of G.

As we will show below, if $|x| = n$ then $\langle x \rangle = \{e, x, \ldots, x^{n-1}\}$ with all elements listed distinct and if $|x| = \infty$ then $\langle x \rangle = \{\ldots, x^{-2}, x^{-1}, e, x, x^2, \ldots\}$ with all elements listed distinct. In the former case $\langle x \rangle = C_n$ and in the latter $\langle x \rangle = C_\infty$, two groups that we will call the cyclic group of order n and infinite cyclic group respectively.

Here is a basic fact we need:

Lemma 1.47. *If $x^m = e$ then $|x| \mid m$.*

Proof. Let $n = |x|$. We have $m = nq + r$ for some $0 \leq r < n$ by the division algorithm. We have $x^r = (x^n)^q x^r = x^m = e$ and so, by the definition of order, it must be that $r = 0$ □

Theorem 1.48. *Let $G = \langle x \rangle$, where x has finite order n. Then*

1. *$|G| = |x| = n$ and $G = \{e, x, \ldots, x^{n-1}\}$.*
2. *If k is an integer, then $|x^k| = \frac{n}{\gcd(k,n)}$. In particular, $\langle x^k \rangle = G$ iff $\gcd(n, k) = 1$.*
3. *There is a bijection*

$$\Psi : \{\text{divisors of } |G|\} \to \{\text{subgroups of } G\} \text{ given by } \Psi(d) = \langle x^{\frac{|G|}{d}} \rangle$$

for each divisor d of $|G|$. Moreover, for each subgroup H of G, $\Psi^{-1}(H) = |H|$. In particular, all subgroups of G are cyclic and there is a unique subgroup of each order.

Proof. 1. By Lemma 1.42, the group G has the following elements $G = \{x^i \mid i \in \mathbb{Z}\}$. We show that

- $|G| \geq n$ by showing the elements $x^0, x^1, \ldots, x^{n-1}$ are distinct. Indeed, if $0 \leq i < j < n$ and $x^i = x^j$ then $x^{j-i} = e$ and $1 \leq j - i < n$, contradicting the minimality of the order of x.
- $|G| \leq n$ by showing $G \subseteq \{x^0, x^1, \ldots, x^{n-1}\}$ (this implies $G = \{e, x, \ldots, x^{n-1}\}$). Indeed, for any $m \in \mathbb{Z}$ division by n yields integers q, r with $0 \leq r \leq n - 1$ such that $m = nq + r$. Then $x^m = x^{nq+r} = (x^n)^q x^r = x^r \in \{x^0, x^1, \ldots, x^{n-1}\}$.

2. Let $y = x^k$, $d = \gcd(n, k)$ and set $n = da, k = db$ for some $a, b \in \mathbb{Z}$ such that $\gcd(a, b) = 1$. We compute $y^a = x^{ka} = x^{dba} = (x^n)^b = e$, so by Lemma 1.47 we have $|y| \mid a$. On the other hand, $x^{k|y|} = y^{|y|} = e$, so again by Lemma 1.47 we have $n \mid k|y|$. Now $n \mid k|y| \iff da \mid k|y| \iff da \mid db|y| \iff a \mid b|y| \iff a \mid |y|$, where the last statement used that $\gcd(a, b) = 1$. Since $a \mid |y|$ and $|y| \mid a$ and $a, |y| > 0$ we conclude $|y| = a = \frac{n}{\gcd(k,n)}$.

3. (See HW 3.) First show that for any $\{e\} \neq H \leq G$, setting $k = \min\{i \mid i \in \mathbb{Z}, i > 0, g^i \in H\}$ gives that $H = \langle g^k \rangle$. Let $\Phi : \{\text{subgroups of } G\} \to \{\text{divisors of } |G|\}$ be the function given by $\Phi(H) = |H|$. Show that Φ is a two sided inverse for Ψ.

□

We can say a little more about the bijection in part 3. of this theorem. Notice how smaller subgroups (with respect to containment) correspond to smaller divisors of G. We can make this observation rigorous by talking about partially ordered set.

Definition 1.49. An *order relation* is a binary relation that is reflexive, antisymmetric ($a \leq b$ and $b \leq a$ imply $a = b$) and transitive. A *partially ordered set* (poset) is a pair $(S, \leq)$ where S is a set endowed with an order relation $\leq$. A *lattice* is a poset in which every two elements have a unique supremum and a unique infimum.

Example. The set of all positive integers is a poset with respect to divisibility ($a \leq b$ iff $a|b$). The supremum of a and b is $\text{lcm}(a, b)$ and the infimum of a and b is $\gcd(a, b)$.

Example. The set of all subsets of a set is a poset with respect to containment ($A \leq B$ iff $A \subseteq B$). The supremum of A and B is $A \cup B$ and the infimum of A and B is $A \cap B$.

Proposition 1.50. *The set of all subgroups of a group G is a lattice with respect to containment.*

Proof. See HW 3. □

Remark 1.51. The isomorphism Ψ in part 3. of Theorem 1.48 satisfies: if $d_1 \mid d_2$ then $\Psi(d_1) \subseteq \Psi(d_2)$. This means that Φ is a *lattice isomorphism* between the lattice of divisors of $|G|$ with division and the lattice of subgroups of G with containment. Ψ^{-1} is also a lattice isomorphism.

Proposition 1.52 (Univeral Mapping Property of a Cyclic Group)**.** *Assume $G = \langle x \rangle$ and let H be any group.*

If $|x| = n < \infty$, then for each $y \in H$ such that $y^n = e$, there is a unique group homomorphism

$$f : G \to H$$

such that $f(x) = y$.

If $|x| = \infty$, then for each $y \in H$, there is a unique group homomorphism

$$f : G \to H$$

such that $f(x) = y$.

In both cases this unique group homomorphism is given by $f(x^i) = y^i$ for any i.

Remark 1.53. This is a particular case of the universal mapping property of a presentation (which we will covered later), since a cyclic group is either presented by $\langle x | x^n = e\rangle$ or $\langle x \mid -\rangle$.

Proof. Recall that either $G = \{e, x, x^2, \dots, x^{n-1}\}$ (with no repetitions) if $|x| = n$ or $G = \{\cdots, x^{-2}, x^{-1}, e, x, x^e, \dots\}$ (with no repetitions) if $|x| = \infty$.

Uniqueness: We show that if $f : G \to H$ is a group homomorphism, then $f(x^i) = y^i$ for all $i \in \mathbb{Z}$.

- if $i = 0$ then $f(x^0) = f(e_G) = e_H = y^0$
- if $i > 0$ then $f(x^i) = f(\underbrace{x \cdots x}_{i \text{ times}}) = \underbrace{f(x) \cdots f(x)}_{i \text{ times}}) = y^i$
- if $i < 0$ then $f(x^i) = f\left((x^{-i})^{-1}\right) = f\left((x^{-i})\right)^{-1} = (y^{-i})^{-1} = y^i$, using the formula above for $-i > 0$

Existence: In either case, define $f(x^i) = y^i$ for all relevant i (i.e., in the first case, for $0 \le i \le n-1$ and in the second for all $i \in \mathbb{Z}$). We need to show this function is a well-defined group homomorphism. To see that f is well defined, suppose $x^i = x^j$ for some $i, j \in \mathbb{Z}$. Then, since $x^{i-j} = e_G$, suing Lemma 1.47 or the definition for order we have

$$\begin{cases} n \mid i-j & \text{if } |x| = n \\ i - j = 0 & \text{if } |x| = \infty \end{cases} \Rightarrow \begin{cases} y^{i-j} = y^{nk} & \text{if } |x| = n \\ y^{i-j} = y^0 & \text{if } |x| = \infty \end{cases} \Rightarrow y^{i-j} = e_H \Rightarrow y^i = y^j.$$

Thus, if $x^i = x^j$ then $f(x^i) = y^i = y^j = f(x^j)$.

The homomorphism property is immediate: $f^(x^i x^j) = f(x^{i+j}) = y^{i+j} = y^i y^j = f(x^i) f(x^j)$. □

Definition 1.54. The *infinite cyclic group* is the group $C_\infty = \{a^i | i \in \mathbb{Z}\}$ with multiplication $a^i a^j = a^{i+j}$. For any natural number n, the *cyclic group of order n* is the group $C_n = \{a^i | i \in \{0, \dots, n-1\}\}$ with multiplication $a^i a^j = a^{i+j \pmod n}$.

The presentations for these groups are $C_\infty = \langle a \mid -\rangle$ and $C_n = \langle a \mid a^n = e\rangle$.

Theorem 1.55 (Classification Theorem for Cyclic Groups)**.** *Every infinite cyclic group is isomorphic to C_∞. Every cyclic group of order n is isomorphic to C_n.*

Proof. Suppose $G = \langle x \rangle$ with $|x| = n$ or $|x| = \infty$ and set $H = C_n$ in the first case and $H = C_\infty$ in the second case. Then by Proposition 1.52, there are homomorphisms $f : G \to H$ and $g : G \to H$ such that $f(x) = a$ and $g(a) = x$. So $g \circ f$ is an endomorphisms of G mapping x to x. But the identity map also has this property, and so the uniqueness clause gives $g \circ f = \mathrm{id}_G$. Similarly, $f \circ g = \mathrm{id}_H$. □

Example. For a fixed $n \geq 1$,

$$\mu_n := \{z \in \mathbb{C} \mid z^n = 1\}$$

is a subgroup of $(\mathbb{C} \setminus \{0\}, \cdot)$. Since $\|z\|^n = \|z^n\|$ and so if $z \in \mu$, then $\|z\| = 1$ and hence $z = e^{ri}$ for some real number r. Moreover, $1 = z^n = e^{nri}$ implies that nr is an integer multiple of 2π. It follows that

$$\mu_n = \{1, e^{2\pi i/n}, e^{4\pi i/n}, \cdots, e^{(n-1)2\pi i/n}\}$$

and that $e^{2\pi i/n}$ generates μ_n. So, μ_n is cyclic or order n. It is therefore isomorphic to C_n, via the map $a^j \mapsto e^{2j\pi i/n}$ for $0 \leq j \leq n-1$.

1.4.3 Subgroups from group actions

Theorem 1.56 (Cayley's Theorem)**.** *Every finite group is isomorphic to a subgroup of S_n.*

Proof. Suppose G is a finite group and label the group elements of G from 1 to n anyway you like. Then the left regular action of G on itself determines a permutation representation $\rho : G \to \mathrm{Perm}(G)$ which gives a bijective group homomorphism $\rho : G \to \mathrm{Im}(\rho)$. Hence $G \cong \mathrm{Im}(\rho)$ and $\mathrm{Im}(\rho)$ is a subgroup of S_n. □

Remark 1.57. This is a nearly useless theorem.

Here are a few more standard examples of subgroups that arise from group actions:

Definition 1.58. If a group G acts on a set S, then for each $s \in S$ and for each $X \subseteq S$ the *pointwise stabilizer* of s, is defined as

$$\mathrm{PtStab}_G(s) = \{g \in G \mid g \cdot s = s\}$$

and the setwise stabilizer of X is defined as

$$\mathrm{SetStab}_G(X) = \{g \in G \mid g \cdot X = X\}, \text{ where } g \cdot X = \{g \cdot x \mid x \in X\}.$$

Exercise. Pointwise and setwise stabilizers are subgroups of G.

Definition 1.59. Suppose that G acts on itself by conjugation. Then for any $x \in G$,

$$C_G(x) := \mathrm{PtStab}_G(x) = \{g \in G \mid gx = xg\}$$

is called the *centralizer* of x in G and for any $X \subseteq G$,

$$N_G(X) := \mathrm{SetStab}_G(X) = \{g \in G \mid gXg^{-1} = X\}$$

is called the *normalizer* of X in G.

1.5 Quotient groups

Recall from your undergraduate algebra course the construction for the integers modulo n: one starts with an equivalence relation $\sim$ on $\mathbb{Z}$, considers the set $\mathbb{Z}/n$ of all equivalence classes with respect to this equivalence relation, and verifies that the operations on $\mathbb{Z}$ give rise to well defined binary operations on the set of equivalence classes.

Does this idea still work if we replace $\mathbb{Z}$ by an arbitrary group? The answer is yes, but one has to be somewhat careful about what equivalence relation is used.

1.5.1 Equivalence relations on a group and cosets

Definition 1.60. An equivalence relation $\sim$ on a group G is compatible with multiplication if whenever $x, y, z \in G$ and $x \sim y$ then $xz \sim yz$ and $zx \sim zy$.

Let $G/\sim$ denote the set of equivalence classes for this relation and write $[g]$ for the equivalence class the an element $g \in G$ belongs to; i.e.

$$[x] := \{g \in G \mid g \sim x\}.$$

Let us ask a question: When does $G/\sim$ aquire the structure of a group under the operation

$$[x] \cdot [y] := [xy] \ ?$$

Right away, we should be worried about whether this operation is independent of choice. That is, if $[x] = [x']$ and $[y] = [y']$ then must $[xy] = [x'y']$? In other words, if $x \sim x'$ and $y \sim y'$, must $xy \sim x'y'$?

Proposition 1.61. *For a group G and equivalence relation $\sim$, the rule $[x] \cdot [y] = [xy]$ is well-defined and makes $G/\sim$ into a group if and only if $\sim$ is compatible with multiplication.*

Proof. The rule $[x] \cdot [y] = [xy]$ is well-defined if and only if whenever $[x] = [x']$ and $[y] = [y']$, then $[x][y] = [x'][y']$, i.e. $[xy] = [x'y']$ if and only if whenever $x \sim x'$ and $y \sim y'$, then $xy \sim x'y'$.

Assume $\sim$ is compatible with multiplication. Then $x \sim x'$ implies $xy \sim x'y$ and $y \sim y'$ implies $x'y \sim x'y'$, hence by transitivity $xy \sim x'y'$.

Conversely, assume the rule $[x] \cdot [y] = [xy]$ is well-defined. Setting $y = y'$ above gives whenever $x \sim x'$ then $xy \sim x'y$. Setting $x = x'$ above gives whenever $y \sim y'$ then $xy \sim xy'$. Hence $\sim$ is compatible with multiplication.

We need to prove that in either of these situations, $G/\sim$ really is a group. This is all easy: for x, y, z we have $[x]\cdot([y]\cdot[z]) = [x]\cdot[yz] = [x(yz)] = [(xy)z] = [xy][z] = ([x][y])[z]$ since G itself is a group. We have $[e_G][x] = [x]$ for all x, so that $G/\sim$ has an identity. Finally, $[x][x^{-1}] = [e_G] = e_{G/\sim}$, so that every element in $G/\sim$ has an inverse. $\square$

Definition 1.62. Let G be a group and let $\sim$ be an equivalence relation on G that is compatible with multiplication. The *quotient group* is the set $G/\sim$ of equivalence classes, with group multiplication $[x]\cdot[y]=[xy]$. (This is a group by Proposition 1.61.)

Example. Let $G=\mathbb{Z}$ and let $\sim$ be $\equiv \pmod{n}$ for some $n\in\mathbb{Z}$, $n\geq 1$. Then

$$(\mathbb{Z},+)/\equiv \pmod{n} = (\mathbb{Z}/n,+).$$

The next lingering question is now: how do we come up with equivalence relations that are compatible with a group's multiplication? We learned that group actions lead to equivalence relations. We will tweak this a little bit and consider a subgroup's action on a group.

Definition 1.63. Let H be a subgroup of a group G. The *left action of H on G* is given by $h\cdot g=hg$ for any $h\in H, g\in G$. The *equivalence relation $\sim_H$* on G induced by the left action of H is given by

$$g\sim_H g' \text{ if and only if } g'=hg \text{ for some } n\in H.$$

The equivalence class of $g\in G$, also called the orbit of g, and also called the *right coset of H in G containing g* is

$$Hg=\{hg\mid h\in H\}.$$

There is also a *left coset of N in G containing g* defined by

$$gH=\{gh\mid h\in H\}.$$

Example. Let $G=\mathbb{Z}$ and $H=\langle n\rangle = n\mathbb{Z}=\{nk\mid k\in\mathbb{Z}\}$. Then $x\sim_{n\mathbb{Z}} y \iff x=y+nk$ for some $k\in\mathbb{Z} \iff x\equiv y \pmod{n}$. Therefore the equivalence relation $\sim_{n\mathbb{Z}}$ is the same as congruence modulo n and the right and left cosets of $n\mathbb{Z}$ in $\mathbb{Z}$ are the congruence classes of integers modulo n.

Lemma 1.64. *Let $H\leq G$. The following facts about left cosets are equivalent for $x,y\in G$:*

1. *x and y belong to the same left coset of H in G,*
2. *$x=yh$ for some $h\in H$,*
3. *$y=xh$ for some $h\in H$,*
4. *$y^{-1}x\in H$,*
5. *$x^{-1}y\in H$,*
6. *$xH=yH$.*

Similarly, the following facts about right cosets are equivalent for $x,y\in G$:

1. *x and y belong to the same right coset of H in G,*

2. *$x = hy$ for some $h \in H$,*

3. *$y = hx$ for some $h \in H$,*

4. *$yx^{-1} \in H$,*

5. *$xy^{-1} \in H$,*

6. *$Hx = Hy$.*

Proof. We only prove the statements about left cosets.

1. $\Rightarrow$ 2. : if x and y belong to the same left coset gH of H in G then $x = gh'$ and $y = gh''$ for some $h', h'' \in H$, so $g = y(h'')^{-1}$ and therefore $x = y(h'')^{-1}h' = yh$ where $h = (h'')^{-1}h' \in H$.

2. $\iff$ 3. : $x = yh$ for some $h \in H \iff y = xh^{-1}$ and $h^{-1} \in H$.

2. $\iff$ 4. : $x = yh$ for some $h \in H \iff y^{-1}x = h \in H$.

4. $\iff$ 5. : $y^{-1}x \in H \iff (y^{-1}x)^{-1} \in H \iff x^{-1}y \in H$.

2. $\Rightarrow$ 6. : Suppose $x = yh$ for some $h \in H$, then by 2. $\Rightarrow$ 3. we also have $y = xh''$ for some $h'' \in H$. Then we have

$$xH = \{xh' \mid h' \in H\} = \{yhh' \mid h' \in H\} \subset yH \text{ and}$$

$$yH = \{yh' \mid h' \in H\} = \{xh''h' \mid h' \in H\} \subset xH,$$

thus $xH = yH$.

6. $\Rightarrow$ 1. : Since $e_G = e_H \in H$, we have $x = xe_G \in xH$ and $y = ye_G \in yH$. If $xH = yH$ then, x and y belong to the same left coset. □

September 12, 2018

Lemma 1.65. *For $H \leq G$, the collection of left cosets of H in G form a partition of G, and similarly for the collection of right cosets. That is,*

- *for all $x, y \in G$, either $xH = yH$ or $xH \cap yH = \emptyset$*
- *$\bigcup_{x \in G} xH = G$,*

and similarly for right cosets. Moreover all left and right cosets have the same cardinality: $|xH| = |Hx| = |H|$ for any $x \in G$.

Proof. Let me prove the assertions for right cosets. Clearly every element g of G belongs to at least one right coset, since $g \in Hg$ (since $e \in H$). We need to show any two cosets are either identical or disjoint: if Hx and Hy share an element, then it follows from 1. $\Rightarrow$ 6. of Lemma 1.64 that $Hx = Hy$. This proves that the right

cosets partition G. To see that all right cosets have the same cardinality as H, define a function

$$\rho : H \to Hg$$

by $\rho(h) = hg$. Clearly ρ is onto and if $\rho(h) = \rho(h')$ then $hg = h'g$ and hence $h = h'$, so that ρ is also one-to-one. □

Example. For $G = D_{2n}$ and $H = \langle s \rangle = \{e, s\}$, the left cosets gH of H in G are

$$\{e, s\}, \{r, rs\}, \{r^2, r^2 s\}, \cdots, \{r^{n-1}, r^{n-1}s\}$$

and the right cosets Hg are

$$\{e, s\}, \{r, r^{-1}s\}, \{r^2, r^{-2}s\}, \cdots, \{r^{n-1}, r^{-n+1}s\}.$$

Note that these lists are *not* the same, but they do have the same length. We have $|G| = 2n$, $|H| = 2$ and $[G : H] = n$ (see Definition 1.68 below for this notation).

Keeping $G = D_{2n}$ but now letting $H = \langle r \rangle$, the left cosets are H and

$$sH = \{s, sr, \ldots, sr^{n-1}\} = \{s, r^{n-1}s, r^{n-2}s, \ldots, rs\}$$

and the right cosets are H and

$$Hs = \{s, r^{n-1}s, r^{n-2}s, \ldots, rs\}.$$

In this case the left and right cosets are exactly the same.

Corollary 1.66 (Lagrange's Theorem)**.** *If G is a finite group and $H \leq G$, then*

$$\begin{aligned} |G| &= |H| \cdot (\textit{the number of left cosets of } H \textit{ in } G) \\ &= |H| \cdot (\textit{the number of right cosets of } H \textit{ in } G). \end{aligned}$$

In particular, $|H|$ is a divisor of $|G|$ and the number of left cosets of H in G is equal to the number of right cosets of H in G.

Proof. See HW 2. □

Corollary 1.67. *If G is a finite group and $g \in G$, then $|g|$ divides $|G|$.*

Proof. Exercise. Consider $H = \langle g \rangle$. □

Definition 1.68. The common number of left or right cosets of a subgroup H in a (finite) group G is denoted as $[G : H]$ and called the *index* of H in G. By Lagrange's theorem, if G is finite then

$$[G : H] = \frac{|G|}{|H|}.$$

1.5.2 Normal subgroups

Definition 1.69. A subgroup N of a group G is *normal* in G, written $N \trianglelefteq G$, if $gNg^{-1} = N$ for all $g \in G$.

Example.

- The trivial subgroups $\{e\}$, G of a group G are normal.
- Any subgroup of an abelian group is normal.
- Any subgroup of index two is normal (see HW 4).
- For any group G, $Z(G) \trianglelefteq G$.
- $A_n \trianglelefteq S_n$ (see HW 3).
- Kernels of group homomorhisms are normal (see HW 4). We will see later that, conversely, all normal subgroups are kernels of group homomorphisms.
- Preimages of normal subgroups are normal, that is, if $f : G \to H$ is a group homomorphism and $K \trianglelefteq H$ then $f^{-1}(K) \trianglelefteq G$ (see HW 4).

Remark 1.70. Being a normal subgroup is not a transitive relation. For example, for

$$V = \{e, (12)(34), (13)(24), (14)(23)\}$$

one can show that $V \trianglelefteq S_4$ and, since V is abelian (all groups with 4 elements are abelian), the subgroup $H = \{e, (12)(34)\}$ is normal in V. But H is *not* normal in S_4, since for example

$$(13)[(12)(34)](13)^{-1} = (32)(14) \notin H.$$

Proposition 1.71. *Let G be a group. An equivalence relation $\sim$ on G is compatible with multiplication if and only if $\sim = \sim_N$ for some normal subgroup $N \trianglelefteq G$.*

Proof. We show

$\Leftarrow$ If $\sim$ is compatible with multiplication then setting $N := \{g \in G | g \sim e\}$ gives $N \trianglelefteq G$ and $\sim = \sim_N$.

To see that $N \trianglelefteq G$, let $n \in N$ and $g \in G$. Since $n \in N$, $n \sim e$, thus $gng^{-1} \sim geg^{-1} \sim e$, which shows that $gng^{-1} \in N$. We have shown that $gNg^{-1} \subseteq N$ for any $g \in G$. To show the opposite containment, notice that for $n \in N$ we can write $n = g(g^{-1}ng)g^{-1} = gn'g^{-1}$ for $n' = g^{-1}ng \in N$.

$\Rightarrow$ If $\sim = \sim_N$ then $\sim$ is compatible with multiplication. Let $x, y, z \in G$ such that $x \sim_N y$. Then $y = nx$ for some $n \in N$, so $yz = nxz$ and

$$zy = znx = zn(z^{-1}z)x = (znz^{-1})zx = n'zx$$

for some $n' \in N$, where the last equality uses the normal subgroup property. We deduce that $yz \sim_N xz$ and $zy \sim_N zx$.

□

Proposition 1.72. *Let N be a subgroup of a group G. The following are equivalent:*

1. $N \trianglelefteq G$
2. $gNg^{-1} \subseteq N$ *for all* $g \in G$.
3. $N_G(N) = G$
4. $gN = Ng$ *for all* $g \in G$.

Proof. Let's show the equivalence of 1. and 2. Assume $gNg^{-1} \subseteq N$ for all g. Let's show that $gNg^{-1} = N$ for all g. If $gNg^{-1} \subseteq N$ for all g, then for all g we have $g^{-1}Ng \subseteq N$ and hence $g(g^{-1}Ng)g^{-1} \subseteq gNg^{-1} \subseteq N$ holds. But $g^{-1}(gNg^{-1})g = \{g^{-1}ghg^{-1}g \mid h \in N\} = N$. So $N \subseteq gNg^{-1} \subseteq N$ holds for all g.

Statements 1. and 3. are equivalent by the definition of the normalizer (Def. 1.59).

As for the equivalence of 1. and 4., it follows from this chain of equivalences which use the Exercise below

$$N \trianglelefteq G \iff gNg^{-1} = N, \forall g \in G \iff gNg^{-1}g = Ng, \forall g \in G \iff gN = Ng, \forall g \in G.$$

□

September 14, 2018

Here is the Exercise used in the proof above

Exercise. IF A, B are subsets of a group G and $g \in G$ then

$$A = B \iff Ag = Bg \iff gA = gB.$$

Definition 1.73. For any normal subgroup N of a group G, the *quotient group* G/N is $G/\sim_N$, where $\sim_N$ is the equivalence relation induced by the left action of N on G. In other words, G/N is the set of right cosets of N in G with multiplication given by $Nx \cdot Ny = N(xy)$. By part 4. of Proposition 1.72, G/N is also the set of left cosets of N in G with multiplication given by $xN \cdot yN = (xy)N$.

Remark 1.74. By Lagrange's Theorem, if G is finite we have $|G/N| = \frac{|G|}{|N|}$.

Example. The *infinite dihedral group* D_∞ is the set $D_\infty = \{r^i, r^i s \mid i \in \mathbb{Z}\}$ with multiplication defined by $(r^i)(r^j) = r^{i+j}, (r^i)(r^j s) = r^{i+j}s, (r^i s)(r^j) = r^{i-j}s$, and $(r^i s)(r^j s) = r^{i-j}$. In other words, D_∞ is the group having presentation

$$D_\infty = \langle r, s \mid s^2 = e, srs = r^{-1} \rangle.$$

Then $\langle r^n \rangle \trianglelefteq D_\infty$ and $D_\infty/\langle r^n \rangle \cong D_{2n}$ via $r\langle r^n \rangle \mapsto r$ and $s\langle r^n \rangle \mapsto s$.

Remark. In the example above both D_∞ and $\langle r^n \rangle$ are infinite but $[D_\infty : \langle r^n \rangle] = |D_\infty / \langle r^n \rangle| = |D_{2n}| = 2n$.

Lemma 1.75. *For any group G and normal subgroup N of G, the map $\pi : G \to G/N$ defined by $\pi(g) = gN$ is a surjective group homomorphism with kernel* $\mathrm{Ker}(\pi) = N$.

Proof. Surjectivity is immediate from the definition. The group homomorphism property follows from the computation below which uses the definition of π and the rule for multiplying cosets in G/N:

$$\pi(gg') = (gg')N = gN \cdot g'N = \pi(g)\pi(g').$$

Finally, using Lemma 1.64, we have $\mathrm{Ker}(\pi) = \{g \in G \mid gN = e_G N\} = N$. □

Corollary 1.76. *A subgroup N of a group G is normal in G if and only if N is the kernel of a homomorphism with domain G.*

1.5.3 The Isomorphism Theorems

We come to the so-called Isomorphism Theorems.

Theorem 1.77 (Universal Mapping Property (UMP) of a Quotient Group)**.** *Let G be a group and N a normal subgroup. If $f : G \to H$ is a homomorphism of groups such that $N \subseteq \mathrm{Ker}(f)$, then*

1. *there exists a unique group homomorphism $\overline{f} : G/N \to H$ such that the composition of $\overline{f}$ and the quotient map $\pi : G \twoheadrightarrow G/N$ is f.*
2. *If f is onto, then $\overline{f}$ is onto.*
3. *Moroever,* $\mathrm{Ker}(\overline{f}) = \mathrm{Ker}(f)/N = \{gN \mid f(g) = e_H\}$.

Proof. 1. If such a $\overline{f}$ exists, it is necessarily unique since $G \twoheadrightarrow G/N$ is onto. In fact, if $f = \pi \circ \overline{f}$ then $\overline{f}$ has to be given by the formula

$$\overline{f}(gN) = f(g).$$

We now need to show that this formula determines a well-defined homomorphism: If $xN = yN$, then $y^{-1}x \in N \subseteq \mathrm{Ker}(f)$ and so $f(y)^{-1}f(x) = e$, whence $f(y) = f(x)$. For any x, y we have

$$\overline{f}(xNyN) = \overline{f}(xyN) = f(xy) = f(x)f(y) = \overline{f}(xN)\overline{f}(yN).$$

2. The formula for $\overline{f}$ given above ensures that $\mathrm{Im}\, f = \mathrm{Im}\, \overline{f}$ hence f is surjective if and only if $\overline{f}$ is surjective.

3. We have $\overline{f}(xN) = e_H$ iff $f(x) = e_H$ iff $x \in \mathrm{Ker}(f)$ iff $xN \in \mathrm{Ker}(f)/N$. If $xN \in \mathrm{Ker}(f)/N$ for some $x \in G$, then $xN = yN$ for some $y \in \mathrm{Ker}(f)$ and hence $x = yz$ for some $z \in N$. Since $N \subseteq \mathrm{Ker}(f)$, we have $x \in \mathrm{Ker}(f)$. □

Example. Let G be any group. For $x, y \in G$, set $[x, y] = xyx^{-1}y^{-1}$. Let G' denote the *commutator subgroup* of G generated by all elements of the form $[x, y]$ for $x, y \in G$. (Some people write G' as $[G, G]$.) Then G' is in fact normal: $G' \trianglelefteq G$.

Now let $f : G \to A$ be any group homomorphism from G to an abelian group A. Since $f([x, y]) = [f(x), f(y)] = e$ for all $x, y \in G$ (since A is abelian), we have that $\mathrm{Ker}(f)$ must contain G'. By the UMP for quotients, we get that f factors as

$$f : G \xrightarrow{\pi} G/G' \xrightarrow{\overline{f}} A$$

for a unique group homomorphism $\overline{f}$.

The grup G/G' is called the *abelianization of* G and the motto is: A homomorhism from a group to an abelian group factors uniquely through the abelianization.

September 17, 2018

Theorem 1.78 (First Isomorphism Theorem)**.** *If $f : G \to H$ is a homomorphism of groups, then* $\mathrm{Ker}(g) \trianglelefteq G$ *and the map $\overline{f}$ defined by the UMP induces an isomorphism*

$$\overline{f} : G/\operatorname{Ker}(f) \xrightarrow{\cong} \operatorname{Im}(f).$$

Proof. By the UMP, there exists a homomorphism $\overline{f}$ such that $\overline{f} \circ \pi = f$, and its kernel consists of just the one element $\mathrm{Ker}(f)/\operatorname{Ker}(f)$ of $G/\operatorname{Ker}(f)$. So $\overline{f}$ is one-to-one, and the image of $\overline{f}$ is clearly the same as the image of f. □

Example. For a field F and integer $n \geq 1$, set $G = \mathrm{GL}_n(F)$. Let $H = \mathrm{SL}_n(F)$, those square matrices with determinant 1. This is a normal subgroup for say $A \in \mathrm{GL}_n(F)$ and $B \in \mathrm{SL}_n(F)$. Then

$$\det(ABA^{-1}) = \det(A)\det(B)\det(A)^{-1} = \det(A)\det(A)^{-1} = 1,$$

so that $ABA^{-1} \in H$. This proves $A\,\mathrm{SL}_n(F)A^{-1} \subseteq \mathrm{SL}_n(F)$.

Let's prove that $\mathrm{GL}_n(F)/\operatorname{SL}_n(F) \cong (F \setminus \{0\}, \cdot)$. The map

$$\det : \mathrm{GL}_n(F) \to (F \setminus \{0\}, \cdot)$$

is a surjective group homomorphism whose kernel is by definition $\mathrm{SL}_n(F)$. Now apply the First Isomorphism Theorem.

To set up the Second Isomorphism Theorem, let's prove some things about a set closely related to the supremum of two subgroups in the subgroup lattice.

Definition 1.79. Let H and K be subgroups of a group and define the set

$$HK = \{hk \mid h \in H, k \in K\}.$$

Exercise 1.80. 1. If $H \leq G$ and $K \leq G$ then $HK \leq G$ if and only if $HK = KH$.

2. If $H \leq G$ and $K \leq G$ and either one of H or K is a normal subgroup then $HK \leq G$ and $HK = KH = \langle H \cup K \rangle$.

The identity $HK = KH$ does not mean that every pair of elements from H and K must commute.

Example. In D_{2n}, let $H = \langle s \rangle$ and $K = \langle r \rangle$. Then $HK = KH = D_{2n}$ but of course r and s do not commute. The fact that $HK = KH$ can also be justified by observing that $K \trianglelefteq D_{2n}$.

Theorem 1.81 (Second Isomorphism Theorem)**.** *Let G be a group, $H \leq G$ and $N \trianglelefteq G$. Then $HN \leq G$, $N \cap H \trianglelefteq H$, $N \trianglelefteq HN$ and there is an isomorphism*

$$\frac{H}{N \cap H} \xrightarrow{\cong} \frac{HN}{N}$$

given by

$$h \cdot (N \cap H) \mapsto hN.$$

Proof. The first two assertions are left as exercises and since $N \trianglelefteq G$ we have $N \trianglelefteq HN$. Define a homomorphism $f : H \to \frac{HN}{N}$ by $f(h) = hN$. This is a homomorphism since it is the composition

$$f : H \hookrightarrow HN \xrightarrow{\pi} \frac{HN}{N}$$

of homomorphisms. f is onto since for all h, n we have $hnN = hN = f(h)$. The kernel of f is $\mathrm{Ker}(f) = \{h \mid hN = N\} = H \cap N$. The result thus follows from the first isomorphism theorem. □

Corollary 1.82. *If H and N are finite subgrups of G and $N \trianglelefteq G$, then $|HN| = \frac{|H| \cdot |N|}{|H \cap N|}$. (In fact this is also true without the requirement that N be normal.)*

Example. For a field F and integer $n \geq 1$, let $G = \mathrm{GL}_n(F)$, $N = SL_n(F)$ and H the set of diagonal invertible matrices. As we known $N \trianglelefteq G$ and its pretty easy to see $H \leq G$. Moreover, $HN = G$ since every invertible matrix A can be written as a product of a diagonal matrix and a matrix of determinant 1. It follows that

$$H/(N \cap H) \cong G/N$$

and since we previously showed that $G/N \cong (F \setminus \{0\}, \cdot)$ we get

$$H/(N \cap H) \cong (F \setminus \{0\}, \cdot).$$

Indeed, it's not hard to see this directly (without using the 2nd Isomorphism Theorem). Note that

$$H \cong (F \setminus \{0\}, \cdot)^{\times n}$$

where the right-hand side denotes a cartesian product of groups. $N \cap H$ consists of those diagonal matrices of determinant 1 and, under this isomorphism, it corresponds

to the subgroup of M of $(F \setminus \{0\}, \cdot)^{\times n}$ consisting of those n-tuples $(x_1, \ldots, x_n)$ with $\prod_i x_i = 1$. We have

$$(F \setminus \{0\}, \cdot)^{\times n}/M \cong (F \setminus \{0\}, \cdot)$$

via the map induced by the map that sends $(x_1, \ldots, x_n)$ to $x_1 \cdots x_n$ (using there First Isomorphism Theorem).

Theorem 1.83 (Third Isomorphism Theorem)**.** *Suppose G is a group, $M \leq N \leq G$, $M \trianglelefteq G$ and $N \trianglelefteq G$. Then $M \trianglelefteq N$, $N/M \trianglelefteq G/M$ and there is an isomorphism*

$$(G/M)/(N/M) \xrightarrow{\cong} G/N$$

given by sending the coset of $(G/M)/(N/M)$ represented by gM to gN.

Proof. The first two assertions are immediate from the definitions.

The kernel of the canonical map $\pi : G \twoheadrightarrow G/N$ contains M and so by the UMP for quotients we get an induced homomorhism

$$\phi : G/M \to G/N$$

with $\phi(gM) = \pi(g) = gN$. Moreover, we know

$$\mathrm{Ker}(\phi) = \mathrm{Ker}(\pi)/M = N/M.$$

Finally apply the First Isomorphism Theorem to ϕ. □

September 19, 2018

Example. Let $G = \mathrm{GL}_n(\mathbb{R})$, $N = \{A \in \mathrm{GL}_n(\mathbb{R}) \mid \det(A) > 0\}$ and $M = \mathrm{SL}_n(\mathbb{R})$. It's not hard to see $N \trianglelefteq G$, it is clear $M \leq N$ and we already know $M \trianglelefteq G$. By the Third Isomorphism Theorem we get

$$\mathrm{GL}_n(\mathbb{R})/N \cong (\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}))/(N/SL_n(\mathbb{R})).$$

Let us analyse the right hand side a bit. Recall $\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \cong (\mathbb{R} \setminus \{0\}, \cdot)$ via the determinant map. Under this isomorphism, $N/SL_n(\mathbb{R})$ corresponds to $(\mathbb{R}_{>0}, \cdot)$. So the right hand is isomorphic to $(\mathbb{R} \setminus \{0\}, \cdot)/(\mathbb{R}_{>0}, \cdot)$. The latter is isomorphic to the two element group $(\pm 1, \cdot)$ via the sign map $x \mapsto x/|x|$.

So, $\mathrm{GL}_n(\mathbb{R})/N \cong (\pm 1, \cdot)$. We could have proven this directly by defining a function $\psi : \mathrm{GL}_n(\mathbb{R}) \to (\pm 1, \cdot)$ by $\psi(A) = \det(A)/|\det(A)|$ and checking that it is a surjective homomorphism with kernel N.

Theorem 1.84 (The Lattice Isomorhism Theorem)**.** *Let G be a group and N a normal subgroup. There is an order-preserving bijection of posets (aka, a "lattice isomorphism")*

$$\Psi : \{\textit{subgroups of } G \textit{ that contain } N\} \xrightarrow{\textit{bijective}} \{\textit{subgroups of } G/N\}$$

given by $\Psi(H) = H/N$ *for* $N \leq H \leq G$*. The inverse is defined for* $\mathcal{H} \leq G/N$ *by*

$$\Psi^{-1}(\mathcal{H}) = \pi^{-1}(\mathcal{H}) = \{x \in G \mid \pi(x) \in \mathcal{H}\}$$

where $\pi : G \twoheadrightarrow G/N$ *is the quotient map. We denote* $\Psi(H) = N/N = \overline{H}$*.*

Then this bijection enjoys the following properties:

1. *(normal) subgroups correspond to normal subgroups i.e.,*
   - $H \leq G$ *iff* $\overline{H} \leq \overline{G}$ *and* $\mathcal{H} \leq \overline{G}$ *iff* $\Psi^{-1}(\mathcal{H}) \leq G$
   - $H \trianglelefteq G$ *iff* $\overline{H} \trianglelefteq \overline{G}$ *and* $\mathcal{H} \trianglelefteq \overline{G}$ *iff* $\Psi^{-1}(\mathcal{H}) \trianglelefteq G$
2. *indices are preserved; i.e.,* $[G : H] = [\overline{G} : \overline{H}]$ *and* $[G : \pi^{-1}(\mathcal{H})] = [\overline{G} : \mathcal{H}]$*.*
3. *supremums and infimums are preserved*
   - $\overline{H} \cap \overline{K} = \overline{H \cap H}$ *and* $\langle \overline{H} \cup \overline{K} \rangle = \overline{\langle H \cup K \rangle}$
   - $\Psi^{-1}(\mathcal{H}) \cap \Psi^{-1}(\mathcal{K}) = \Psi^{-1}(\mathcal{H} \cap \mathcal{K})$ *and* $\langle \Psi^{-1}(\mathcal{H}) \cup \Psi^{-1}(\mathcal{K}) \rangle = \Psi^{-1}\left(\langle \mathcal{H} \cup \mathcal{K} \rangle\right)$

Proof. We have previously shown that the quotient map $\pi : G \to G/N$ is a surjective group homomorphism. It will be useful to rewrite the maps in the statement of the theorem in terms of π.

Notice that $\Psi(H) = H/N = \{hN \mid h \in H\} = \pi(H)$ and define a new map

$$\Phi : \{\text{subgroups of } G/N\} \to \{\text{subgroups of } G \text{ that contain } N\}$$

by $\Phi(\mathcal{H}) = \pi^{-1}(\mathcal{H})$ for any $\mathcal{H} \leq G/N$.

We show:

- Ψ is well defined (correct codomain) since for $H \leq G$ we have $\pi(H) \leq G/N$ (since images of subgroups through group homomorphisms are subgroups).
- Φ is well defined (correct codomain) since for $\mathcal{H} \leq G$ we have $\pi^{-1}(\mathcal{H}) \leq G$ (since preimages of subgroups through group homomorphisms are subgroups) and for any $\mathcal{H} \leq G$ we have $\{e_G N\} \subseteq \mathcal{H}$, hence

  $$N = \text{Ker}(\pi) = \pi^{-1}(\{e_G N\}) \subseteq \pi^{-1}(\mathcal{H}) = \Phi(\mathcal{H}).$$

- Φ and Ψ are mutual inverses:
  $(\Psi \circ \Phi)(\mathcal{H}) = \pi(\pi^{-1}(\mathcal{H})) = \mathcal{H}$ since π is surjective and
  $(\Phi \circ \Psi)(H) = \pi^{-1}(\pi(H)) = \pi^{-1}(H/N) = H$, with the last equality justified by

  $$\begin{aligned} x \in \pi^{-1}(H/N) &\iff \pi(x) \in H/N \iff xN = hN \text{ for some } h \in H \\ &\iff x \in hN \text{ for some } h \in H \iff x \in H \text{ (using that } N \subseteq H). \end{aligned}$$

Thus, the two functions defined in the statement are well-defined and are mutually inverse. Since π and π^{-1} preserve containments, each of Ψ, Ψ^{-1} preserves the order relation of containment.

I will only prove some parts of statements (1), (2), (3) in the theorem.

(1) If $N \leq H \leq G$ and $H \trianglelefteq G$, then $H/N \trianglelefteq G/N$ holds by part of the 3rd Isomorphism Theorem or by the exercise below, since π is surjective. The fact that the inverse function also sends normal subgroups to normal subgroups is a consequence of the statement that inverse images of normal subgroups are normal subgroups (see HW 4).

(2) In the interest of time, I'll only prove the assertion about indices in the special case when H is normal. In that case this fact is also an immediate consequence of the Third Isomorhism Theorem since for $N \leq H \leq G$ with $H \trianglelefteq G$ we have

$$[G : H] = |G/H| = |(G/N)/(H/N)| = [G/N : H/N] = [\overline{G} : \overline{H}].$$

The general case is a consequence of an exercise from HW 5.

(3) is a consequence of the more general fact that lattice isomorphisms preserve supremums and infimums. □

Exercise 1.85. If $f : G \to H$ is a group homomorphism and $K \trianglelefteq G$ then $f(K) \trianglelefteq f(G)$. In particular, if f is surjective then $f(K) \trianglelefteq H$ (but this need not be true in the absence of surjectivity, see HW 4).

September 21, 2018

1.5.4 Presentations as quotient groups

We can finally define group presentations in a completely rigorous manner.

Definition 1.86. Let A be a set. Consider a new set of symbols $A^{-1} = \{a^{-1} \mid a \in A\}$. The *free group* on A, denoted $F(A)$, is the set of all finite words written using symbols in $A \cup A^{-1}$, including the empty word, where two words are equal if one is obtained from the other by erasing a pair of consecutive symbols aa^{-1} or $a^{-1}a$. In symbols,

$$F(A) = \{a_1^{i_1} a_2^{i_2} \cdots a_m^{i_m} \mid m \geq 0, a_j \in A, i_j \in \{-1, 1\}\}.$$

The set $F(A)$ is a group in which any two words are multiplied by concatenation.

Example. The free group on a singleton set $A = x$ is the infinite cyclic group C_∞.

Theorem 1.87 (Universal mapping property for free groups)**.** *Let A be a set, let $F(A)$ be the free group on A, let H be a group, and let $g : A \to H$ be a function. Then there is a unique homomorphism $f : F(A) \to H$ satisfying $f(a) = g(a)$ for all $a \in A$.*

Proof. Set $f : F(A) \to H$ to be given by $f(a_1^{i_1}a_2^{i_2}\cdots a_m^{i_m}) = g(a_1)^{i_1}g(a_2)^{i_2}\cdots g(a_m)^{a_m}$ for any $m \geq 0, a_j \in A, i_j \in \{-1, 1\}$. One checks that f is well defined by noting that

$$f(a_1^{i_1}a_2^{i_2}\cdots aa^{-1}\cdots a_m^{i_m}) = g(a_1)^{i_1}g(a_2)^{i_2}\cdots g(a)g(a)^{-1}\cdots g(a_m)^{a_m} = f(a_1^{i_1}a_2^{i_2}\cdots a_m^{i_m})$$

for any $a \in G$ and similarly for inserting $a^{-1}a$. The fact that f is a group homomorphism and its uniqueness are left as an easy exercise. □

Definition 1.88. Let G be a group and let $R \subseteq G$ be a set. The *normal subgroup of G generated by R*, denoted $\langle R\rangle^N$, is the set of all products of conjugates of elements of R and inverses of elements of R. In symbols,

$$\langle R\rangle^N = \{g_1r_1^{i_1}g_1^{-1}\ldots g_mr_m^{i_m}g_m^{-1} \mid m \geq 0, r_j \in R, g_j \in G, i_j \in \{1, -1\}, \forall 1 \leq j \leq m\}.$$

Definition 1.89. Let A be a set and let R be a subset of the free group $F(A)$. The group with *presentation* $\langle A \mid R\rangle = \langle A|\{r = e \mid r \in R\}\rangle$ is defined to be the quotient group $F(A)/\langle R\rangle^N$.

Example. For $A = \{x\}$, $R = \{x^n\}$ we obtain the cyclic group of order n:

$$C_n = \langle x \mid x^n = e\rangle = \frac{F(\{x\})}{\langle x^n\rangle^N} = C_\infty/\langle x^n\rangle.$$

Example. For $A = \{r, s\}$, $R = \{s^2, r^n, srsr\}$ we obtain the usual presentation for D_{2n}:

$$D_{2n} = \langle r, s \mid s^2 = e, r^n = e, srsr = e\rangle = \frac{F(\{r, s\})}{\{s^2, r^n, srsr\}^N}.$$

Theorem 1.90 (Universal mapping property of a presentation)**.** *Let A be a set, let $F(A)$ be the free group on A, let R be a subset of $F(A)$, let H be a group, and let $g : A \to H$ be a function satisfying the property that whenever $r = a_1^{i1}\cdots a_m^{i_m} \in R$, with each $a_j \in A, g_j \in G$ and $i_j \in \{1, -1\}$, then $(g(a_1))^{i_1}\cdots(g(a_m))^{i_m} = e_H$. Then there is a unique homomorphism $\overline{f} : \langle A|R\rangle \to H$ satisfying $\overline{f}(a\langle R\rangle^N) = g(a)$ for all $a \in A$.*

Proof. By the UMP of the free group there is a unique group homomorphism $\tilde{f} : F(A) \to H$ such that $f(a) = g(a)$ for all $a \in A$. Then for $r = a_1^{i1}\cdots a_m^{i_m} \in R$, we have $f(r) = (g(a_1))^{i_1}\cdots(g(a_m))^{i_m} = e_H$, showing that $R \subseteq \mathrm{Ker}(f)$. Since $\mathrm{Ker}(f) \trianglelefteq F(A)$ and $\langle R\rangle^N$ is the smallest normal subgroup containing R, it follows that $\langle R\rangle^N \subseteq \mathrm{Ker}(f)$. By the UMP of the quotient, f induces a group homomorphism $\overline{f} : G/\langle R\rangle^N \to H$. Moreover, for each $a \in A$ we have $g(a) = f(a) = \overline{f}(a\langle R\rangle^N)$. □

Remark. The UMP of the presentation says that one can build a homomorphism from a group with a given presentation to any other group H as long as one is able to send the generators (elements of A) via some function g to some elements of H that satisfy the same relations in H as those given in the presentation.

Example. To find a groups homomorphism $D_{2n} \to \mathrm{GL}_2(\mathbb{R})$ it suffices to find a map $g : \{r, s\} \to \mathrm{GL}_2(\mathbb{R})$, say $r \mapsto R, s \mapsto S$ and to verify that $S^2 = I_2, R^n = I_2, SRSR = I_2$. As you have shown on homework, this does hold for the matrices

$$S = \begin{bmatrix} \cos 2\pi n & -\sin 2\pi n \\ \sin 2\pi n & \cos 2\pi n \end{bmatrix}, R = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

By the UMP of the presentation there is a group homomorphism $D_{2n} \to \mathrm{GL}_2(\mathbb{R})$ that extends g.

Spetember 24, 2018

1.6 More group actions

1.6.1 S_n acting on polynomials and the alternating group A_n

Let $x_1, \ldots, x_n$ be n variables and let $F[x_1, \ldots, x_n]$ denote the set of all polynomials with coefficients in a field F and variables $x_1, \ldots x_n$.

For any polynomial $g(x_1, \ldots, x_n)$ and any $\sigma \in S_n$, set

$$(\sigma \cdot g)(x_1, \ldots, x_n) = g(x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

It is clear that $e_{S_n} \cdot g = g$ and slightly less clear but still true that $(\tau \cdot (\sigma \cdot g)) = (\tau \circ \sigma) \cdot g$. Thus S_n acts on $F[x_1, \ldots, x_n]$ via this rule. Even better, this rule is compatible with the addition and multiplication of polynomials, so we have

$$\sigma \cdot (g + f) = (\sigma \cdot g) + (\sigma \cdot f)\sigma \text{ and } \sigma \cdot (gf) = (\sigma \cdot g)(\sigma \cdot f).$$

Lemma 1.91. *For any n, define a polynomial with real coefficients*

$$P = P(x_1, \ldots, x_n) = \prod_{1 \le i < j \le n} (x_i - x_j).$$

Then for any $\sigma \in S_n$ we have

$$\sigma \cdot P = \pm P.$$

Example. If $n = 3$, $P = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$.

If $n = 4$, $P = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4)$.

Proof. Using that the action preserves products of polynomials, we get

$$\sigma \cdot P = \prod_{i<j} (x_{\sigma(i)} - x_{\sigma(j)}),$$

and thus $\sigma \cdot P$ and P are products of the same list of linear factors, up to a sign. $\square$

Definition 1.92. For $\sigma \in S_n$, define $\text{sign}(\sigma) \in \{\pm 1\}$ so that the equation

$$\sigma \cdot P = \text{sign}(\sigma) P$$

holds. In other words,

$$\text{sign}(\sigma) := \frac{\sigma \cdot P}{P}.$$

Remark 1.93. Since

$$\sigma \cdot P = \prod_{i<j} (x_{\sigma(i)} - x_{\sigma(j)})$$

the sign of σ is $(-1)^m$ where m is the number of linear factors in which the variables occur in the wrong order in $\sigma \cdot P$. That is,

$$\text{sign}(\sigma) = (-1)^m \text{ where } m = \#\{(i,j) \mid i < j, \sigma(i) > \sigma(j)\}.$$

Example. If $\sigma = (1\,2)$ then for any n we have

$$P = (x_1 - x_2)(x_1 - x_3) \cdots (x_1 - x_n) \cdot (x_2 - x_3)(x_2 - x_4) \cdots (x_2 - x_n) \cdot \prod_{3 \le i < j \le n} (x_i - x_j)$$

and

$$\sigma \cdot P = (x_2 - x_1)(x_2 - x_3) \cdots (x_2 - x_n) \cdot (x_1 - x_3)(x_1 - x_4) \cdots (x_1 - x_n) \cdot \prod_{3 \le i < j \le n} (x_i - x_j).$$

Thus $\text{sign}((1\,2)) = -1$.

Proposition 1.94. *For $n \ge 2$, the function* sign $: S_n \to \{\pm 1\}$ *is a group homomophism.*

Proof. For $\alpha, \beta \in S_n$, we have

$$\text{sign}(\alpha) = \beta \cdot \text{sign}(\alpha) = \beta \cdot \left(\frac{\alpha \cdot P}{P} \right) = \frac{\beta \cdot (\alpha \cdot P)}{\beta \cdot P} = \frac{(\beta\alpha) \cdot P}{P} \frac{P}{\beta \cdot P} = \frac{\text{sign}(\beta\alpha)}{\text{sign}(\beta)}$$

and hence

$$\text{sign}(\beta\alpha) = \text{sign}(\beta)\text{sign}(\alpha).$$

This shows that sign is a homomorphism. □

Definition 1.95. The kernel of the sign homomorphism is a subgroup of S_n denoted A_n and called the *alternating group.*

Proposition 1.96. *For $n \ge 2$, A_n is a normal subgroup of S_n of index 2. A_n is the collection of permutations in S_n that can be written as a product of an even number of transpositions.*

Proof. Observe that sign is an onto group homomorphism with kernel A_n. Because kernels are normal subgroups, A_n is normal and because $S_n/A_n \cong \{\pm 1\}$ it follows that $[S_n : A_n] = 2$.

By the previous example, the sign of a transposition is -1 and since sign is a homomorphism we deduce that the sign of a product of transpositions is -1 to the number of transpositions. In particular, $\sigma \in A_N \iff \text{sign}(\sigma) = 1$ if and only if σ can be written as a product of an even number of transpositions. □

1.6.2 Groups action basics: LOIS

One of the most important facts about the action of a group on a finite set is "LOIS". Recall that for an element $s \in X$ the orbit of s is

$$\text{Orbit}_G(s) = \{g \cdot s \mid g \in G\}$$

and the stabilizer is

$$\text{Stab}_G(s) = \{g \in G \mid g \cdot s = s\}.$$

The stabilizer $\text{Stab}_G(s)$ is a subgroup of G.

Theorem 1.97 (LOIS = The Length of the Orbit is the Index of the Stabilizer)**.** *Let G be a group that acts on a finite set S via $\cdot$. For any $s \in S$ we have*

$$|\,\text{Orbit}_G(s)| = [G : \text{Stab}_G(s)]$$

Proof. This is a direct consequence of LOIS. □

Proof. Let $\mathcal{L}$ be the collection of left cosets of $\text{Stab}_G(s)$ in G. Define a function

$$\alpha : \mathcal{L} \to \text{Orbit}_G(s)$$

by $\alpha(x\,\text{Stab}_G(s)) = x \cdot s$. This function is well defined and one-to-one:

$$x\,\text{Stab}_G(s) = y\,\text{Stab}_G(s) \iff x^{-1}y \in \text{Stab}_G(s) \iff x^{-1}y \cdot s = s \iff y \cdot s = x \cdot s.$$

The function α is onto by definition of $\text{Orbit}_G(s)$. □

September 26, 2018

Corollary 1.98 (Orbit-Stabilizer Theorem)**.** *Let G be a group that acts on a finite set S via $\cdot$. For any $s \in S$ we have*

$$|G| = |\,\text{Orbit}_G(s)| \cdot |\,\text{Stab}_G(s)].$$

Recall from previous chapters the following terminology related to group actions.

Definition 1.99. A *permutation representation* of a group G is a homomorphism $\rho : G \to \text{Perm}(S)$ for some set S.

By Proposition 1.34, for a group G acting on a set S, there is a permutation representation $\rho : G \to \text{Perm}(S)$ induced by the action.

Definition 1.100. An action is *faithful* if the only element $g \in G$ such that $g \cdot s = s$ for all $s \in S$ is $g = e_G$. Equivalently an action is faithful if $\text{Ker}(\rho) = \{e_G\}$.

Definition 1.101. An action is *transitive* if for all $p, q \in S$ there is a $g \in G$ such that $q = g \cdot p$. Equivalently, an action is transitive if $\text{Orbit}_G(p) = S$ for any $p \in S$.

Example. Let G be the group of rotational (orientation-preserving) symmetries of the cube. There is a faithful homomorphism from G to S_4 given by the action of G on the four lines that join opposite vertices of the cube. It turns out that this homomorphism is actually an isomorphism from G to S_4 as one can see that the action is faithful (hence the permutation representation $G \to S_4$ is injective) and the two groups have the same cardinality. To count the number of elements of G, think about an isometry as picking up a cube lying on a table and replacing it in the same location. To do this, one must pick a face to place on the table. This can be chosen in 6 ways. Once that face is chosen, one needs to decide on where each vertex of that face goes and this can be done in 4 ways. Thus $|G| = 24 = |S_4|$.

Let G act on the collection of 6 faces of the cube. This action is transitive and so the one and only orbit has length 6. It follows that for any face f of the cube, G_f has index 6 and, since we already know that $|G| = 24$, it follows from LOIS that $|\operatorname{Stab}_G(f)| = 4$. That is, there are four symmetries that map f to itself. Indeed, they are the 4 rotations by 0, 90, 180 or 270 degrees about the line of symmetry passing through the mid-point of f and the mid-point of the opposite face.

1.6.3 Groups acting on their cosets by left multiplication

Theorem 1.102. *Let H be a subgroup of a group G. Then G acts on the set G/H of left cosets by left multiplication $g(g'H) = (gg')H$. Furthermore*

1. *the action is transitive*
2. *$\operatorname{Stab}_G(1_{G/H}) = H$ and*
3. *if ρ is the induced permutation representation, then $\operatorname{Ker}(\rho) = \bigcap_{g\in G} gHg^{-1}$ is the largest normal subgroup of G contained in H.*

Proof. We only prove parts 1. and 3.

For 1. notice that for any $g, h \in G$ we have $(hg^{-1})gH = hH$.

For 3. we have

$$\begin{aligned}
\operatorname{Ker}(\rho) &= \{x \in G \mid xgH = gH \text{ for all } g \in G\} \\
&= \{g \in G \mid g^{-1}xgH = H \text{ for all } g \in G\} \\
&= \{g \in G \mid g^{-1}xg \in H \text{ for all } g \in G\} \\
&= \{g \in G \mid x \in\in gHg^{-1} \text{ for all } g \in G\} \\
&= \bigcap_{g\in G} gHg^{-1}.
\end{aligned}$$

Because any kernel is a normal subgroup, $\operatorname{Ker}(\rho) \trianglelefteq G$ and because H is one of the sets being intersected in the displayed formula above, $\operatorname{Ker}(\rho) \subseteq H$. Let $K \trianglelefteq G$ and $K \subseteq H$. Then $K = gKg^{-1}$ for any $g \in G$, so we have that

$$K = \bigcap_{g\in G} gKg^{-1} \subseteq \bigcap_{g\in G} gHg^{-1} = \operatorname{Ker}(\rho).$$

This shows that $\mathrm{Ker}(\rho)$ is the largest normal subgroup contained in H. $\square$

Theorem 1.103. *If G is a finite group of order n and p is the smallest prime dividing $|G|$, then any subgroup H of G of index p is normal in G.*

Proof. Let $S = G/H$ and note that $|S| = p$. Let $K = \bigcap_{g \in G} gHg^{-1}$ be the kernel of the permutation representation $G \to \mathrm{Perm}(S)$. By the first isomorphism theorem we have $G/K \cong \mathrm{Im}(\rho) \leq \mathrm{Perm}(S)$. Thus, by Lagrange's Theorem

$$|G/K| \mid p!. \tag{1}$$

Since $K \leq H$, we have that $[G : K] = [G : H][H : K]$, so denoting $[H : K] = k$ we have

$$[G : K] = pk. \tag{2}$$

Putting the two equations together yields $k \mid (p-1)!$, thus if k has any prime factors, they are all smaller than p. By a corollary to Lagrange's theorem $k = [H : K]$ divides $|H|$ which in turn divides $|G|$. Since $|G|$ has no prime factors smaller than p it follows that $k = 1$ and thus $H = K \trianglelefteq G$. $\square$

September 28, 2018

1.6.4 Groups acting on themselves by conjugation

Let G be a group. We know from previous sections that G acts on G by conjugation, where this action is defined by the rule $g \cdot x = gxg^{-1}$.

Definition 1.104. Let G be a group. Two elements $g, g' \in G$ are *conjugate* if there is $h \in G$ with $g' = hgh^{-1}$ (equivalently g and g' are in the same orbit of the conjugation action).

The *conjugacy class* of an element $g \in G$ is $[g]_c = \{hgh^{-1} \mid h \in G\}$, i.e. the orbit of g under conjugation.

Two subsets $S, S' \subseteq G$ are conjugate if there is $h \in G$ with $S' = hSh^{-1}$.

We will study conjugation in symmetric groups specifically.

Proposition 1.105. *Two elements of S_n are conjugate if and only if they have the same cycle type.*

First a Lemma:

Lemma 1.106. *For $\sigma \in S_n$ and distinct intgers $i_1, \ldots, i_p$ we have*

$$\sigma(i_1\, i_2 \cdots i_p)\sigma^{-1} = (\sigma(i_1) \cdots \sigma(i_p)).$$

(Note that the right-hand cycle is a cycle since σ is one-to-one.)

Proof. To prove this, evaluate both sides at $\sigma(i_t)$ for any t and observe that one gets $\sigma(i_{t+1})$ (with the supscript taken modulo p) both times. This proves they agree on the set $\sigma(\{i_1, \ldots, i_p\})$. If j is not in this set, then $(i_1\, i_2\, \cdots i_p)$ fixes $\sigma^{-1}(j)$ so the left-hand side fixes j. So does the right, since $\sigma^{-1}(j) \notin \{\sigma(i_1), \ldots, \sigma(i_p)\}$. Thus the two functions coincide on elements. □

Proof of Proposition. If two elements of S_n are conjugate, say $\beta = \sigma\alpha\sigma^{-1}$, then they have the same cycle type, since we may write α as a product of disjont cycles $\alpha = \alpha_1 \cdots \alpha_m$ and then apply the Lemma. Indeed, $\sigma\alpha\sigma^{-1} = (\sigma\alpha_1\sigma^{-1}) \cdots (\sigma\alpha_m\sigma^{-1})$ and the Lemma shows that the right-side is a product of disjoint cycles.

Conversely, suppose $\alpha = \alpha_1 \cdots \alpha_k$ and $\beta = \beta_1 \cdots \beta_k$ are decompositions into disjoint cycles and that α_i, β_i both have length $p_i \geq 2$ for all i. We need to prove α and β are conjugate. Let's start with the case $k = 1$: given two cycles of the same length

$$\alpha = (i_1 \ \ldots \ i_p) \text{ and } \beta = (j_1 \ \ldots \ j_p).$$

If σ is any permulation such that $\sigma(i_m) = j_m$ for all $m = 1, \ldots, p$, then $\sigma\alpha\sigma^{-1} = \beta$ by the Lemma.

Note that such σ is "allowed" to map $\{1, \ldots, n\} \backslash \{i_1 \ \ldots \ i_p\}$ bijectively to $\{1, \ldots, \} \backslash \{j_1 \ \ldots \ j_p\}$ in any way possible. From this observation the general case follows: since the cycles are disjoint, we can find a single permutation σ such that $\sigma\alpha_i\sigma^{-1} = \beta_i$ for all i. □

Example. The conjugacy classes for S_4 are

1. $\{e\}$,
2. all two cycles of which there are $\binom{4}{2} = 6$,
3. all three cycles of which there are $4 \cdot 2 = 8$,
4. all four cycles of which there are $3! = 6$, and
5. all product of two disjoint two cycles of which there are 3.

This totals 24, as we need, since the conjugacy classes partition S_4.

Lemma 1.107. *Let $N \trianglelefteq G$. The conjugation action of G on itself induces an action by conjugation of G on N. On particular, N is the disjoint union of some of the conjugacy classes in G.*

Proof. Define the conjugation action of G on N by $g \cdot n = gng^{-1}$ for all $g \in G$ and $n \in N$. Since $N \trianglelefteq G$ this is well defined. The two properties in the definition of the action hold for the action of G by conjugation on N since they hold more generally for the action of G by conjugation on G. Therefore this is indeed an action. The orbits of elements $n \in N$ under this action are $[n]_c$. Thus the conjugacy classes of the elements of N partition N. □

Example. One thing we get from the previous example and lemma is a very short list of all possible sizes of normal subgroups of S_4. Here's why:

An important, general observation is that, any group G and $N \trianglelefteq G$, since $gNg^{-1} = N$ for all g, it follows that N is necessarily a union of conjugacy classes. In other words, the action of G on itself by conjugation restricts to an action on N since N is normal, and thus N is a union of orbits of this action. Moreover, if G is finite then, by Lagrange, $|N| \mid |G|$. Finally, N certainly contains e. Putting these facts together we get than $|N|$ must both divide $|G|$ and be a sum of cardinalities of conjugacy classes, including the class $\{e\}$.

For example, if $N \trianglelefteq S_4$, then $|N| \mid 24$ and $|N|$ must equal 1 plus the sum of some sub-list of $6, 8, 6, 3$. The only possibilities are

$$1, 1+3, 1+3+8, 1+6+8+6+3$$

The first and last represent the boring normal subgroups: $\{e\}$ and G. $1+3$ also represents a normal subgroup, which consists of all the products of all product of two disjoint two cycles and the identity:

$$V = \{e, (12)(34), (13)(24), (14)(23)\}.$$

The last one exists too and it is A_4.

October 8, 2018

Recall from Definition 1.59 that for any $g \in G$,

$$C_G(g) := \{g \in G \mid gx = xg\}$$

is called the *centralizer* of g in G and for any $S \subseteq G$,

$$N_G(S) := \{g \in G \mid gSg^{-1} = S\}$$

is called the *normalizer* of S in G.

Theorem 1.108. *Let G be a group.*

1. *Then G acts on G by conjugation ($gg' = gg'g^{-1}$). For all $g \in G$, the orbit of g is the conjugacy class of g, $\mathrm{Stab}_G(g) = C_G(G)$ and $|[g]_c| = |G : C_G(g)|$.*
2. *Then G acts on the power set $P(G) = \{S \mid S \subseteq G\}$ by conjugation ($gS = gSg^{-1}$). For all $S \in P(G)$, $\mathrm{Stab}_G(S) = N_G(S)$ and $|\mathrm{Orbit}_G(S)| = |G : N_G(S)|$.*

Proof. It all follows from definitions and LOIS. □

Corollary 1.109. *For a finite group G, the size of any conjugacy class divides $|G|$.*

Cutoff point for the midterm exam.

Theorem 1.110 (The Class Equation)**.** *Let G be a finite group and let $g_1, \dots g_r \in G$ be a list of unique representatives of all of the conjugacy classes of G of size greater than 1. Then*

$$|G| = |Z(G)| + \sum_i^r |G : C_G(g_i)|$$

.

Proof. The elements of $Z(G)$ are precisely the group elements that are conjugate to only themselves; that is, they are the one-element orbits for the conjugation action. Because the conjugacy classes (orbits of the conjugation action) partition G we have

$$|G| = |Z(G)| + \sum_i^r [g_i]_c.$$

For each g_i as in the statement, by Theorem 1.108, we have $[G : C_G(g_i)] = [g_i]_c$. The class equation follows from substituting this into the equation above. □

Definition 1.111. For a prime number p, a p-group is a group of order p^m for some $m \in \mathbb{Z}, m > 0$.

Corollary 1.112. *If p is a prime number and G is a finite group of order p^m for some $m > 0$, then $Z(G)$ is not the trivial group.*

Proof. Let $g_1, \dots g_r \in G$ be a list of unique representatives of all of the conjugacy classes of G of size greater than 1 as in the class equation. Then for each i, $C_G(g_i) \neq G$ so $[G : C_G(g_i)] \neq 1$. Since $1 \neq [G : C_G(g_i)] \mid |G| = p^m$, it follows that $p \mid [G : C_G(g_i)]$ for each i. From the Class equation we deduce that $p \mid |Z(G)|$ so, $|Z(G)| \neq 1$. □

Example. Let us analize the conjugacy classes of A_5.

Since $A_5 \leq S_5$, we know that *if* two elements of A_5 are conjugate, *then* they have the same cycle type. But there is no reason for the converse to hold for observe that given $\alpha, \beta \in A_5$ of the same cycle type, the elements $\sigma \in S_5$ that give $\sigma\alpha\sigma^{-1} = \beta$ might all belong to $S_5 \setminus A_5$. Indeed, this does happen in some cases.

The possible cycle types of elements of A_5 are

1. five cycles, of which there are $4! = 24$,
2. three cycles, of which there are $\binom{5}{3}2 = 20$,
3. products of two disjoint transpositions, of which there are $5 \cdot 3 = 15$, and
4. $\{e\}$,

Let's start with five cycles. Let $\sigma = (1\,2\,3\,4\,5)$. We have by Theorem 1.108 (a) that

$$C_{C_5}(\sigma) = \frac{C_5}{|\text{ conjugacy class of } \sigma \text{ in } S_5|} = \frac{5!}{4!} = 5.$$

This yields that the centralizer of σ *in* S_5 is

$$C_{S_5}(\sigma) = \{e, \sigma, \sigma^2, \sigma^3, \sigma^4\},$$

since the five listed permutations do commute with σ and there can be no more elements in $C_{S_5}(\sigma)$ because of cardinality reasons. Moreover, it is obvious from the definitions that

$$C_{A_5}(\sigma) = C_{S_5}(\sigma) \cap A_5$$

and so we conclude that

$$C_{A_5}(\sigma) = \{e, \sigma, \sigma^2, \sigma^3, \sigma^4\}$$

too. Thus, by LOIS,

$$\text{the size of the conjugacy class of } \sigma \text{ in } A_5 = [A_5 : C_{A_5}(\sigma)] = 60/5 = 12.$$

That is, σ is only conjugate in A_5 to half of the five cycles.

If we pick a five cycle σ' that is not conjugate in A_5 to σ, the same reasoning shows that σ' is conjugate to exactly 12 elements, which must be exactly the other 12 five cycles. It is not hard to see that in fact $(1\,2\,3\,4\,5)$ and $(2\,1\,3\,4\,5)$ are not conjugate. In a bit more detail, they *are* conjugate *in* S_5 via the element $(1\,2)$. From this one sees that the only elements α in S_5 such that

$$\alpha(1\,2\,3\,4\,5)\alpha^{-1} = (2\,1\,3\,4\,5)$$

holds are members of the coset $C_{S_5}(\sigma) \cdot (1\,2)$, which contains no elements of A_5.)

October 10,2018

So far we know the following about the conjugacy classes of A_5:

1. the conjugacy class of $(1\,2\,3\,4\,5)$ has 12 elements,
2. the conjugacy class of $(2\,1\,3\,4\,5)$ has 12 elements, and this class is distinct from the previous one, and
3. the collection of all three cycles, of which there are 20, forms one or more conjugacy classes,
4. the collection of all products of two disjoint transpositions, of which there are 15, forms one or more conjugacy classes.
5. $\{e\}$ is a conjugacy class,

Given two three cycles $(a\,b\,c)$ and $(d\,e\,f)$, there is a $\sigma \in S_5$ such that

$$\sigma(a\,b\,c)\sigma^{-1} = (d\,e\,f).$$

If σ is not in A_5, then let x, y be the two elements of $\{1, \ldots, 5\} \setminus \{a, b, c\}$. Then we have

$$(\sigma \cdot (x\,y))(a\,b\,c)(\sigma \cdot (x\,y))^{-1} = (d\,e\,f).$$

and $\sigma \cdot (x\,y) \in A_5$.

To figure out what's going on the in last case, set $\alpha = (1\,2)(3\,4)$. Because the cardinality of the conjugacy class of α in S_5 is 15 (it consists of all the products of two disjoint two-cycles) we get

$$15 = |[\alpha]_{c \text{ in } S_5}| = [S_5 : C_{S_5}(\alpha)] = \frac{120}{|C_{S_5}(\alpha)|} \Rightarrow |C_{S_5}(\alpha)| = 8.$$

Since

$$C_{A_5}(\alpha) = C_{S_5}(\alpha) \cap A_5,$$

it follows that $\#C_{A_5}(\alpha)$ must divide both 8 and 60, and so must be one of $1, 2$ or 4. Since α commutes with e, α, $(1\,3)(2\,4)$ and $(1\,4)(2\,3)$ and each of these belongs to A_5, we must have $\#C_{A_5}(\alpha) = 4$. It follows that α is conjugate to $60/4 = 15$ elements – i.e., α must be conjugate in A_5 to all elements of its cycle type.

We conclude that the conjugacy classes of A_5 are given by the following list:

1. the conjugacy class of $(1\,2\,3\,4\,5)$ has 12 elements,
2. the conjugacy class of $(2\,1\,3\,4\,5)$ has 12 elements, and this class is distinct from the previous one,
3. the collection of all three cycles, of which there are 20, forms a conjugacy class,
4. the collection of all products of two disjoint transpositions, of which there are 15, forms one conjugacy class, and
5. $\{e\}$ is a conjugacy class.

Theorem 1.113. *A_5 is a simple group.*

Proof. Suppose $N \trianglelefteq A_5$. Then $\#N \mid 60$ and

$$\#N = 1 + \text{ the sum of a sub-list of the list } 20, 12, 12, 15.$$

By checking the relatively small number of cases we see that $\#N = 1$ or $\#N = 60$ are the only possibilities. □

1.6.5 Sylow Theory

We come to a very powerful technique for analyzing finite groups of relatively small order. One aspect of Sylow theory is that it allows us to deduce, in certain special cases, the existence of a unique subgroup of a given order, and thus it allows one to construct a normal subgroup.

Let's start with a couple of facts covered on the homework

Lemma 1.114. *Suppose G is a group and m is a positive integer. Then*

1. *If $H \leq G$ is a subgroup of order m, then $gHg^{-1} \leq G$ is a subgroup of order m.*
2. *If there is a unique subgroup H of G of order m, then $H \trianglelefteq G$.*

Because of part 2. of Lemma 1.114 if m is any integer, then G acts on the set $\mathcal{S}$ consisting of all subgroups of G of order m. (It could be the empty set.) Moreover, if $H \in \mathcal{S}$, then by Theorem 1.108 the stabilizer of this action is

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\} = \text{ the } \textit{normalizer} \text{ of } H \text{ in } G.$$

Moroever, $H \trianglelefteq G$ iff $N_G(H) = G$.

Definition 1.115. Let G be a finite group and p a prime. Write the order of G as $\#G = p^e m$ where $p \nmid m$. A *Sylow p-subgroup* of G is a subgroup $H \leq G$ such that $\#H = p^e$.

That is, a Sylow p-subgroup of G is a subgroup whose order is the highest conceivable power of p according to Lagrange's Theorem. We set $\mathrm{Syl}_p(G)$ to be the collection of all Sylow p-subgroups of G and $n_p = |\mathrm{Syl}_p(G)|$ to be the number of Sylow p-subgroups.

Remark 1.116. We allow the case when $p \nmid |G|$, in which case $e = 0$ and G has a unique Sylow p-suubgroup, namely $\{e\}$ which has order p^0.

Example. In D_{2p} for a prime p, $\langle r \rangle$ is a Sylow p-subgroup. If $p > 2$, there is only one Sylow p-subgroup of D_{2p}, so $n_p = 1$.

In D_{2n} for n odd, each of the subgroups $\langle sr^j \rangle$, for $j = 0, \ldots, n-1$ is a Sylow 2-subgroup, so $n_2 = p$.

Example. Thanks to Colby for catching a mistake in a previous version of this example. In S_5, the Sylow 5-subgorups are the cyclic groups $\langle \sigma \rangle$ for any five cycle σ, so $n_5 = 6$ because there are 24 five cycles, but there are four of these in every Sylow 5-subgroup. The Sylow 3-subgorups are the cyclic groups $\langle \sigma \rangle$ for any three cycle σ, so $n_3 = 10$ because there are 20 three cycles, but there are two of these in every Sylow 3-subgroup.

A Sylow 2-subgroup of S_5 is any subgroup of order 8. For example $\langle (1\,4)(2\,3), (1\,2\,3\,4) \rangle$ is a Sylow 2-subgroup. There are many others.

Note that if G is a finite group and p is a prime with $p \mid G$, then G acts on its Sylow p-subgroups via conjugation. (As of now, for all we know, this might be the action on the empty set.) Sylow Theory is all about understanding this action very well. Let's jump in and state the main Theorem. Then we'll apply it to examples, before proving it later on.

Theorem 1.117 (Main Theorem of Sylow Theory)**.** *Assume G is a group of order $p^e m$ where p is prime, $e \geq 0$, and $\gcd(p, m) = 1$.*

1. $\mathrm{Syl}_p(G) \neq \emptyset$ *(there exists at least one Sylow p-subgroup of G).*

2. *If P is a Sylow p-subgroup of G and $Q \leq G$ is any p-subgroup of G (i.e., a subgroup whose order is some power of p), then there is a g such that $Q \leq gPg^{-1}$. In particular, the action of G on $\mathrm{Syl}_p(G)$ by conjugation is transitive — i.e., any two Sylow p-subgroups are conjugate.*

3. *We have*
$$|\mathrm{Syl}_p(G)| \equiv 1 \mod p.$$

4. *For any $P \in \mathrm{Syl}_p(G)$,*
$$|\mathrm{Syl}_p(G)| = [G : N_G(P)],$$
and hence
$$|\mathrm{Syl}_p(G)| \mid m.$$

October 12, 2018

Sylow's main theorem ic closely related to Cauchy's Theorem.

Theorem 1.118 (Cauchy's Theorem)**.** *If G is a finite group and p is a prime number dividing $|G|$, then G has an element of order p. (In fact, at least $p-1$ elements of order p.)*

Proof. See HW 6. □

Remark 1.119. In general, Cauchy's Theorem can be deduced from part one of the Sylow Theorem. For say $p \mid \#G$. Then there exists a Sylow p-subgroup P of G. Pick any $x \in P$, $x \neq e$. Then $|x| = p^j$ for some $j \geq 1$. Then $x^{p^{j-1}}$ has order p.

However, we will use (a more restrictive form of) Cauchy's Theorem to prove Sylow's Theorem, so it is important to see that Cauchy's Theorem can be proven independently of Sylow theory.

Example. Let us prove that no group or order 12 is simple. Let G be any group of order 12. We will prove that G must have either a normal subgroup of order 3 or a normal subgroups of oder 4.

Sylow theory gives that $n_2 = |\mathrm{Syl}_2(G)|$ is either 1 or 3 and $n_3 = |\mathrm{Syl}_3(G)|$ is either 1 or 4. If either of these numbers is 1, we have a unique subgroup of order 4 or of order 3, and such a subgroup must be normal. Suppose these numbers are 3 and 4, respectively. We deduce a contradition by "counting elements".

In detail, say $P_1, \ldots, P_4$ are the 4 Sylow 3-subgroups. By Lagrange $P_i \cap P_j = \{e\}$ for all $i \neq j$. Thus the *set* $T := \bigcup_{i=1}^4 P_i$ has 9 elements, one of which is e and the other 8 of which must have order 3. That is, there are 8 elements of order 3 in G. But now consider the three Sylow 2-subgroups Q_1, Q_2, Q_3. Each has order 4 and $Q_i \cap T = \{e\}$ for all i. It follows that $Q_i = \{e\} \cup (G \setminus T)$ for all i, and thus $Q_1 = Q_2 = Q_3$, a contradiction.

Warning: In the previous example, it would not be so easy to count elements of order 2 and 4. We do know that every element in $S := \cup_i Q_i$ has order 1, 2 or 4 (any only one has order 1), but the size of this set is harder to calculate. For notice that $Q_i \cap Q_j$ might have order 2. The most one can say for sure is that S has at least $4 + 4 - 2 = 6$ elements.

Proof of Part (1) of the Sylow Theorem. Recall that we write $|G| = p^e m$ where $p \nmid m$. We need to prove G contains a subgroup of order p^e, and we proceed by induction on $|G|$.

If $|G| = 1$ or, more generally, if $p \nmid |G|$, then $\{e\}$ is a Sylow p-subgroup. We may thus assume $p \mid |G|$. We proceed by considering two cases, depending on whether or not p divides $|Z(G)|$.

If $p \mid |Z(G)|$, then by Cauchy's Theorem, there is an element $z \in Z(G)$ of order p. Set $N = \langle z \rangle$. Since $z \in Z(G)$, we have $N \trianglelefteq G$. Since $|G/N| = p^{e-1}m$, by induction G/N has a subgroup of order p^{e-1} (i.e. of index m). By the Fourth Isomorphism Theorem, this subgroup corresponds to a subgroup of G of index m, hence of order p^e.

For the second case, assume $p \nmid |Z(G)|$ and consider the class equation for G:

$$|G| = |Z(G)| + \sum_{i=1}^{k} [G : C_G(g_i)]$$

where $g_1, \ldots, g_k$ are a complete and non-redundant list of non-central conjugacy class representatives. Since $p \nmid |Z(G)|$ and $p \mid |G|$, we must have $p \nmid [G : C_G(g_i)]$ for at least one i. For this i, we have $|C_G(g_i)| = p^e j$ where $p \nmid j$. Since g_i is not central, $|C_G(g_i)| < |G|$ and hence, by induction, $C_G(g_i)$ contains a subgroup of order p^e. But this subgroup is also a subgroup of G. □

Remark 1.120. I mentioned that Cauchy's Theorem is a consequence of part (1) of the Sylow Theorem, but we have used Cauchy in the proof here. Notice, however, that we only need Cauchy for *abelian groups* in this proof, and that is easier to prove.

Example. No group of order $80 = 5 \cdot 16$ is simple.

By way of contradicton suppose G is simple and $|G| = 80$. Sylow theory gives $|\operatorname{Syl}_2(G)| = 5$ and $|\operatorname{Syl}_5(G)| = 16$ (since they cannot be 1 by the assumption that G is simple). The "counting elements trick" would work, but let's proceed in a different way: Consider the action of G on $\operatorname{Syl}_2(G)$ by conjugation and let

$$\rho : G \to S_5$$

be the associated permutation representation (obtained by choosing a numbering $1, \ldots, 5$ of the members of $\operatorname{Syl}_2(G)$). The map ρ is non-trivial since the action is transitive by part (2) of the Sylow Theorem. But 80 does not divide 120 and so ρ cannot be injective. It follows that $\operatorname{Ker}(\rho)$ is a non-trivial, proper normal subgroup of G, a contradiction.

October 17, 2018

The proofs of other parts of the Sylow Theorem require a technical lemma:

Lemma 1.121. *Let G be a finite group, p a prime, P a Sylow p-subgroup of G, and Q any p-subgroup of G. Then $Q \cap N_G(P) = Q \cap P$.*

Proof. Since $P \leq N_G(P)$, we have $Q \cap P \leq Q \cap N_G(P)$. For the reverse containment, let $H = Q \cap N_G(P)$. Since $H \subseteq N_G(P)$, we have that $PH = HP$ so PH is a subgroup of G by Exercise 1.80. Also by Corollary 1.82 we have

$$|PH| = \frac{|P||H|}{|P \cap H|}$$

and since each of $|P|$, $|H|$, and $|P \cap H|$ is a power of p, PH is a p-subgroup of G. But $P \leq PH$ and P is a p-subgroup of largest possible order. So $P = PH$. This proves $H \leq P$ and thus $H \leq Q \cap P$. □

Proof of Parts (2) and (3) of the Sylow Theorem. Let P be a Sylow p-subgroup and let Q be any p-subgroup. Let $\mathcal{S}_P$ denote the collection of all conjugates of P:

$$\mathcal{S}_P = \{gPg^{-1} \mid g \in G\}.$$

Part (3) tells us the $\mathcal{S}_P$ consists of all Sylow p-subgroups of G, but we don't yet know this. Nonetheless, G acts (transitively) on $\mathcal{S}_P$ by conjugation, and thus Q also acts on $\mathcal{S}_P$ (not necessarily transitively). The key to proving parts (2) and (3) of the Sylow Theorem is to analyse the action of Q on $\mathcal{S}_P$ to establish (1.6.1) and (1.6.2) below.

Let $O_1, \ldots, O_s$ be the orbits of the action of Q on $\mathcal{S}_P$, and for each i pick a representative $P_i \in O_i$. We have $\text{stab}_Q(P_i) = \{q \in Q \mid qP_iq^{-1} = P_i\} = Q \cap N_G(P_i) = Q \cap P_i$, where the last equation uses the Lemma. By LOIS, we thus have $|O_i| = [Q : Q \cap P_i]$ and hence

$$|\mathcal{S}_P| = \sum_{i=1}^{s} [Q : Q \cap P_i] \tag{1.6.1}$$

This equation holds for any p-subgroup Q of G. In particular, we can take $Q = P_1$. In this case the first term is 1 and, since $Q \cap P_i = P_1 \cap P_i < P_1 = Q$ for all $i \neq 1$, the remaining terms are divisible by p. This gives

$$|\mathcal{S}_P| \equiv 1 \pmod{p}. \tag{1.6.2}$$

(This does not yet prove part (3) since we don't yet know that $\mathcal{S}_P$ consists of all Sylow p-subgroups.)

We can now prove part (2): By way of contradiction, suppose Q is a p-subgroup of G such that Q is not contained in any of the subgroups belonging to $\mathcal{S}_P$. Then $Q \cap P_i < Q$ for all i and thus every term on the right-hand side of (1.6.1) is divisble by p, contrary to (1.6.2). The second assertion in (2) follows by taking Q to be a Sylow p-subgroup.

This proves, in particular, that $\mathcal{S}_P$ in fact does consist of all Sylow p-subgroups. Part (3) thus follows from (1.6.2). □

Proof of Part (4) of the Sylow Theorem. This is really immediate from the previous parts: For any $P \in \mathrm{Syl}_p(G)$, the stablizer of P for the action of G on $\mathrm{Syl}_p(G)$ by conjugation is $N_G(P)$. Since we now know the action is transitive,

$$|\mathrm{Syl}_p(G)| = [G : N_G(P)].$$

Moreover, since $P \leq N_G(P)$ and $|P| = p^e$, it follows that $[G : N_G(P)] \mid m$. □

October 19, 2018

1.7 Direct and semidirect products, the FTFGAG

We now discuss how to build new groups from old ones.

1.7.1 Direct products

Definition 1.122. Let G_α be a group for all α in an index set J. The *direct product* of the groups G_α is the Cartesian product $\prod_{\alpha\in J} G_\alpha$ with multiplication defined by

$$(g_a)_{\alpha\in J}(h_\alpha)_{\alpha\in J} = (g_\alpha h_\alpha)_{\alpha\in J}.$$

The *direct sum* of the groups G_α is the subset $\bigoplus_{\alpha\in J} G_\alpha$ of the direct product $\prod_{\alpha\in J} G_\alpha$ given by

$$\bigoplus_{\alpha\in J} G_\alpha = \{(g_\alpha)_{\alpha\in J} \mid g_\alpha = e_{G_\alpha} \text{ for all but finitely many } \alpha\},$$

with the same multiplication as the direct product.

Theorem 1.123. *The direct product of a collection of groups is a group, and the direct sum of the collection is a subgroup of the direct product.*

Proof. Exercise. □

Example. If $\gcd(m, n) = 1$ then $\mathbb{Z}/m \times \mathbb{Z}/n \cong \mathbb{Z}/mn$. Indeed consider the elements $x = (1, 0)$ and $y = (0, 1)$ in $\mathbb{Z}/m\times\mathbb{Z}/n$. Then $|x| = m, |y| = n$ and $x+y = y+x = (1, 1)$. Therefore $|xy| = \mathrm{lcm}(|x|, |y|) = mn$. Since $\langle x+y\rangle \subseteq \mathbb{Z}/m \times \mathbb{Z}/n$ and both of these sets have cardinality mn it must be the case that $\mathbb{Z}/m \times \mathbb{Z}/n = \langle x + y\rangle = \langle(1, 1)\rangle$. Since $\langle x + y\rangle$ and $\mathbb{Z}/mn$ are both cyclic groups of order mn they are isomorphic. Thus

$$\mathbb{Z}/m \times \mathbb{Z}/n \cong \mathbb{Z}/mn.$$

Theorem 1.124 (Recognition theorem for direct products)**.** *Suppose G is a group with normal subgroups $H \trianglelefteq G$ and $K \trianglelefteq G$ such that $H \cap K = \{e\}$ Then $HK \cong H \times K$ via the isomorphism of groups $\theta : H \times K \to HK$ defined by $\theta(h, k) = hk$. Moreover $H \cong \theta^{-1}(H) = \{(h, e) \mid h \in H\} \leq H \times K$ and $K \cong \theta^{-1}(K) = \{(e, k) \mid k \in K\} \leq H \times K$.*

Proof. Notice that the hypothesis implies $HK \leq G$. Furthermore $H \trianglelefteq G, K \trianglelefteq G$ and $H \cap K = \{e\}$ imply that the elements of H commute with the elements of K. Indeed, consider $h \in H, k \in K$. Then since $H \trianglelefteq G$, $khk^{-1} \in H$, so also $[k,h] = khk^{-1}h^{-1} \in H$. Similarly it follows that $[k,h] \in K$, but since $H \cap K = \{e\}$ it follows that $[k,h] = e$, i.e. $hk = kh$ for any $h \in H, k \in K$.

Using the above we have

$$\begin{aligned}\theta((h_1,k_1)(h_2,k_2)) &= \theta(h_1h_2, k_1k_2)\\ &= h_1h_2k_1k_2\\ &= h_1k_1h_2k_2 = \theta(h_1,k_1)\theta(h_2,k_2)\end{aligned}$$

and thus θ is a homomorphism. It's kernel is $\{(k,h) \mid k = h^{-1}\}$, which is just $\{e\}$ since $H \cap K = \{e\}$. The image of θ is clearly HK. This proves θ is an isomorphism. □

Definition 1.125. If $H \trianglelefteq G$ and $K \trianglelefteq G$ are such that $H \cap K = \{e\}$ then we call HK is called the *internal direct product* of H and K and $H \times K$ the *external direct product* of H and K.

We now discuss an important generalization for the direct product and a new method of constructing a new groups from the action of one group on another.

Suppose G is a group with subgroups $H \trianglelefteq G$ and $K \leq G$ such that $H \cap K = \{e\}$. Then we still have $HK \leq G$; let's see what we would need the multiplication on the cartesian product $H \times K$ to be in order for $\theta : H \times K \to HK$ defined by $\theta(h,k) = hk$ to still be a group homomorphism:

$$\theta(h_1,k_1)\theta(h_2,k_2) = h_1k_1h_2k_2 = h_1h_2'k_1k_2 = \theta(h_1h_2', k_1k_2),$$

where $h_2' \in H$ is such that $k_1h_2k_1^{-1} = h_2'$.

This means that we would need to have $(h_1,k_1)(h_2,k_2) = (h_1h_2', k_1k_2)$ for θ to be a homomorphism. This motivates the following definition.

1.7.2 Semidirect products

Definition 1.126. Let H and K be groups and let $\rho : K \to \mathrm{Aut}(H)$ be a homomorphism. The (external) *semidirect product* induced by ρ is the set $H \times K$ with the binary operation defined by

$$(h,k)(h',k') = (h\rho(k)(h'), kk').$$

This group is denoted by $H \rtimes_\rho K$.

Before we prove that the construction above actually gives a group, let's compute a few examples.

Example. Given H and K we could always take ρ to be the trivial homomorphism, so that $\rho(y)(x) = x$ for all $y \in K$ and $x \in H$. Then $K \rtimes_\rho H$ is just the usual direct product:

$$(y_1, x_1)(y_2, x_2) = (y_1 y_2, x_1 x_2).$$

Example. Fix a group G, a normal subgroup $H \trianglelefteq G$ and a subgroup $K \leq G$. Then the function

$$\rho : K \to \mathrm{Aut}(H)$$

given by $\rho(x)(y) = xyx^{-1}$ for $x \in K, y \in H$ is a homomorphism. Thus K acts on H via automorphisms.

Example. Let $K = \langle x \rangle$ be cyclic of order 2 and $H = \langle y \rangle$ be cyclic of order n for any $n \geq 1$. As described in HW 7, $\mathrm{Aut}(H) \cong (\mathbb{Z}/n)^\times$.

In particular, -1 is an element of $(\mathbb{Z}/n)^\times$, for any $n \geq 1$, and the associated automorphism sends y to y^{-1}. This automorphism is clearly its own inverse; i.e., it has order 2. Therefore, by the UMP for cyclic groups, there is a homomorphism

$$\rho : K \to \mathrm{Aut}(H)$$

with $\rho(x)(y) = y^{-1}$. We may thus form the group

$$G := H \rtimes_\rho K.$$

The elements of G are (y^i, x^j) for $0 \leq i \leq n-1$ and $0 \leq j \leq 1$, in particular $|G| = 2n$. Set

$$\tilde{y} = (y, e) \in G \text{ and } \tilde{x} = (e, x) \in G$$

Then

$$\tilde{y}^n = (y, e_K)^n = (y^n, e_K) = (e_H, e_K) = e_G$$
$$\tilde{x}^2 = (e_H, x)^2 = (e_H, x^2) = (e_H, e_K) = e_G$$

and

$$\tilde{x}\tilde{y}\tilde{x}\tilde{y} = (e_H, x)(y, e_K)(e_H, x)(y, e_K) = (\rho(x)(y), x)(\rho(x)(y), x) = (y^{-1}, x)(y^{-1}, x) = (y^{-1}y, e) = e_G.$$

Looks familar!

Indeed, by the universal mapping property for D_{2n} we have a homomorphism

$$\theta : D_{2n} \to G$$

such that $\theta(r) = (y, e_K)$ and $\theta(s) = (x, e_H)$. Moreover, θ is onto since

$$\theta(r^i s^j) = (y^i, x^j) \text{ for all } 0 \leq i \leq n-1, 0 \leq j \leq 1$$

and since $|D_{2n}| = |G| = 2n$ it follows that θ is a bijection. So the dihedral group is a semidirect product, in which the two component groups are cyclic of orders n and 2 respectively:

$$D_{2n} \cong \langle y \rangle \rtimes_\rho \langle x \rangle$$

and ρ is the inversion homomorphism as described above.

October 24, 2018

Theorem 1.127. *If H and K are groups and $\rho : K \to \mathrm{Aut}(H)$ is a homomorphism, then setting :*

1. *$H \rtimes_\rho K$ is a group*
2. *$H \cong H' := \{(h, e) \mid h \in H\} \trianglelefteq H \rtimes_\rho K$ and $K \cong K' := \{(e, k) \mid k \in K\} \leq H \rtimes_\rho K$*
3. *$(H \rtimes_\rho K)/H' \cong K$.*

Proof. (1.) The proof is straightforward but a bit messy. For associativity, note that

$$\begin{aligned}(y_1, x_1)\left((y_2, x_2)(y_3, x_3)\right) &= (y_1, x_1)(y_2\rho(x_2)(y_3), x_2x_3) = \left(y_1\rho(x_1)\left(y_2\rho(x_2)(y_3)\right), x_1x_2x_3\right)\\ &= (y_1\rho(x_1)(y_2)(\rho(x_1)\circ\rho(x_2))(y_3), x_1x_2x_3)\\ &= (y_1\rho(x_1)(y_2)\rho(x_1x_2)(y_3), x_1x_2x_3)\end{aligned}$$

On the other hand

$$\left((y_1, x_1)(y_2, x_2)\right)(y_3, x_3) = (y_1\rho(x_1)(y_2), x_1x_2)(y_3, x_3) = (y_1\rho(x_1)(y_2)\rho(x_1x_2)(y_3), x_1x_2x_3).$$

This gives associativity.

The fact that (e, e) is a two-sided identity follows from the fact that $\rho(e)(y) = \mathrm{id}_H(y) = y$.

Finally

$$\begin{aligned}(y, x)(\rho(x^{-1})(y^{-1}), x^{-1}) &= \left(y\rho(x)\left(\rho(x^{-1})(y^{-1})\right), e\right) = (y(\rho(x)\circ\rho(x^{-1}))(y^{-1}), e)\\ &= (y\rho(e)(y^{-1}), e) = (yy^{-1}, e) = (e, e),\end{aligned}$$

and similarly

$$(\rho(x^{-1})(y^{-1}), x^{-1})(y, x) = (e, e).$$

(2.) Define a funtion

$$i : H \to H \rtimes_\rho K$$

as $i(y) = (y, e)$. Then i is a homomorphism, since

$$i(y_1)i(y_2) = (y_1, e)(y_2, e) = (y_1\rho(e)(y_2), ee) = (y_1y_2, e) = i(y_1y_2).$$

The map is clearly injective and hence its image is isomorphic to H. In fact, the image is normal since the second component of

$$(y, x)(y_2, e)(\rho(x^{-1})(y^{-1}), x^{-1})$$

is clearly e. Let us write this image as

$$H' := \{(y, e) \mid y \in H\} \trianglelefteq H \rtimes_\rho K.$$

The function

$$j : K \to H \rtimes_\rho K$$

defined by $j(x) = (e, x)$ is also an injective homomorphism and thus its image

$$K' := \{(e, x) \mid x \in H\} \leq H \rtimes_\rho K$$

is isomorphic to K. K' is typically *not* normal, however. Finally, it is easy to see that $H'K' = H \rtimes_\rho K$ and $H' \cap K' = \{e\}$. Putting this all together we have

- $H' \trianglelefteq H \rtimes_\rho K$,
- $K' \leq H \rtimes_\rho K$,
- $H'K' = H \rtimes_\rho K$, and
- $H' \cap K' = \{e\}$.

(3.) Consider the projection onto the second factor $\pi_2 : H \rtimes_\rho K \to K$ given by $\pi_2(y, x) = x$. This is a goup homomorphism since the second component of $(y_1, x_1)(y_2, x_2)$ is x_1x_2 and is surjective by definition. Now

$$\mathrm{Ker}(\pi_2) = \{(y, e_K) \mid y \in H\} = H' \cong H.$$

By the first isomorphism theorem we conclude that $(H \rtimes_\rho K)/H' \cong K$.

□

Exercise 1.128. If we idenify K with K' and H with H' via the isomorphisms i and j, prove the action of H' on K' via conjugation in $K \rtimes_\rho H$ coincides with the original action ρ.

We can turn this around.

Proposition 1.129 (Recognition theorem for internal semidirect products)**.** *For a group G, suppose we are given H and K so that*

- $H \trianglelefteq G$,
- $K \leq G$,
- $HK = G$, *and*
- $H \cap K = \{e\}$.

Let $\rho : K \to \mathrm{Aut}(H)$ be the permutation representation of the action of K on H via automorphisms given by conjugation in G. (This means that for any $k \in K$ $\rho(k) = c_k$, where $c_k \in \mathrm{Aut}(H)$ is the function $c_k(h) = khk^{-1}$ for all $h \in H$.) Then the function

$$\theta : H \rtimes_\rho K \to G$$

defined by $\theta(y, x) = yx$ is an isomorphism of groups.

Moreover, under this isomorphism, K corresponds to K' and H corresponds to H' (referring to the notation in Theorem 1.127 above).

Proof. We have

$$\begin{aligned}\theta((y_1, x_1)(y_2, x_2)) &= \theta(y_1 c_{x_1}(y_2), x_1 x_2) \\ &= y_1 x_1 y_2 x_1^{-1} x_1 x_2 \\ &= y_1 x_1 y_2 x_2 = \theta(y_1, x_1)\theta(y_2, x_2)\end{aligned}$$

and thus θ is a homomorphism. It's kernel is $\{(y, x) \mid y = x^{-1}, y \in H, x \in K\}$, which is just $\{e\}$ since $H \cap K = \{e\}$. The image of θ is clearly $KH = G$. This proves θ is an isomorphism. It is obvious that $\theta(K') = K$ and $\theta(H') = H$. □

Definition 1.130. In this situation of the Proposition 1.129, we will say that G is the *internal semi-direct product* of H and K.

Example. Returning to D_{2n}, let $H = \langle s \rangle$ and $K = \langle r \rangle$. Then $H \leq G$, $K \trianglelefteq G$, $HK = G$ and $H \cap K = \{e\}$. So, G is isomorphic to a semi-direct product, as we already showed.

Example. Let $G = S_n$, $K = A_n$ and $H = \langle (1\,2) \rangle$. Then $K \trianglelefteq G$, $H \leq G$, $KH = G$ and $K \cap H = \{e\}$. It follows that

$$S_n \cong A_n \rtimes_\rho C_2$$

where $C_2 = \langle x \rangle$ is cyclic of order 2 and the action $\rho : C_2 \to \mathrm{Aut}(A_n)$ sends x to conjugation by $(1\,2)$.

October 26, 2018

It is important to be aware that for a fixed pair of groups H and K, different actions of H on K via automorphisms can result in isomorphic semi-direct products. Indeed, determining when $K \rtimes_\rho H \cong K \rtimes_{\rho'} H$ is in general a tricky business. The previous example shows this:

Example. Let $G = S_n$ and $K = A_n$ again, but this time take $H' = \langle (1\,3) \rangle = (1\,2\,3)\langle (1\,2) \rangle (1\,2\,3)^{-1}$ (assuming $n \geq 3$). Then we get

$$S_n \cong A_n \rtimes_{\rho'} C_2$$

where $C_2 = \langle x \rangle$ is cyclic of order 2 and the action $\rho' : C_2 \to \mathrm{Aut}(A_n)$ sends x to conjugation by $(1\,3)$.

The actions ρ and ρ' are not identical. For example,

$$\rho(x)(1\,2) = (1\,2)$$

and

$$\rho'(x)(1\,2) = (2\,3).$$

Yet

$$A_n \rtimes_\rho H \cong A_n \rtimes_{\rho'} H'$$

since each is isomorphic to S_n.

On HW 9 you will give a more conceptual reason for why these two semidirect products turned out to be isomorphic: it is because H and H' are conjugate in S_n.

1.7.3 Classification for finite groups of small order

We can now combine the ideas from Sylow theory, (semi)direct products and the classification theorem for finitely generated abelian groups (yet to be stated) to classify the isomorphism classes of groups of smaall order.

We start with a baby example.

Example. Any group of order 6 is isomorphic either to $\mathbb{Z}/6$ or to D_6.

Proof. Let G be a group of order 6. Cayley's theorem gives that there exist elements $x, y \in G$ with $|x| = 2$ and $|y| = 3$. Let $K = \langle x \rangle$ and $H = \langle y \rangle$. Since $[G : H] = 2$, H is a normal subgroup of G and since $H \cap K$ is a common subgroup of H and K Lagrange's theorem gives that $|H \cap K| \mid \gcd(|H|, |K|) = 1$. Thus $H \cap K = \{e\}$ and since $|HK| = \frac{|H||K|}{|H \cap K|} = 6 = |G|$ we deduce that $HK = G$. Proposition 1.129 now gives that G is the internal semidirect product of H and K. More to the point, $G \cong H \rtimes_\rho K$, where $\rho : K \to \mathrm{Aut}(H)$ gives the action of K on H by conjugation.

We now analyze the possibilities for ρ. By a HW problem, $\mathrm{Aut}(H) \cong \mathrm{Aut}(\mathbb{Z}/3) \cong (\mathbb{Z}/3^\times, \cdot) = (\{\pm 1\}, \cdot)$. There are two possibilities for the image of ρ: either $\mathrm{Im}(\rho) = \{\mathrm{id}_H\}$ or $\mathrm{Im}(\rho) = \mathrm{Aut}(H)$.

If $\mathrm{Im}(\rho) = \{\mathrm{id}_H\}$, then $\rho(x) = c_x = \mathrm{id}_H$ (which implies $xy = yx$) and $H \rtimes_\rho K = H \times K$. Therefore, in this case $G \cong H \times K \cong \mathbb{Z}/3 \times \mathbb{Z}/2 \cong \mathbb{Z}/6$, where the last isomorphism uses the Chinese Remainder Theorem 1.140.

If $\mathrm{Im}(\rho) = \mathrm{Aut}(H)$, then $\rho(x)$ is the map $y^i \mapsto y^{-1}$ and by an earlier example for this ρ we have $H \rtimes_\rho K \cong D_6$, so $G \cong D_6$.

Finally, $\mathbb{Z}/6 \ncong D_6$ because the former is abelian and the latter is not. □

We will find the following facts very useful for this type of problems.

Exercise 1.131. Let K be a finite cyclic group and let H be an arbitrary group. Suppose that the images of $\phi : K \to \mathrm{Aut}(H)$ and $\theta : K \to \mathrm{Aut}(H)$ are conjugate subgroups of $\mathrm{Aut}(H)$. Then $H \rtimes_\phi K \cong H \rtimes_\theta K$.

Exercise 1.132. $\mathrm{Aut}(\underbrace{\mathbb{Z}/p \times \cdots \times \mathbb{Z}/p}_{n \text{ factors}}) \cong GL_n(\mathbb{F}_p)$ and these groups have order $(p^n-1)(p^n-p)(p^n-p^2)\cdots(p^n-p^{n-1})$.

Example. Let's repeat the previous example for classifying groups of order 55 into isomorphism classes.

If $|G| = 55$, then by Cauchy G contains an element x of order 5 and an element y or order 11. Let $K = \langle y \rangle$ and $H = \langle x \rangle$. Then $[G : K] = 5$ and hence $K \trianglelefteq G$, using Theorem 1.103. By Lagrange $H \cap K = \{e\}$ and by counting $HK = G$. Thus

$$G \cong K \rtimes_\rho H$$

for some action $\rho : H \to \mathrm{Aut}(K)$. Since K is cyclic of order 11, we know $\mathrm{Aut}(K) \cong (\mathbb{Z}/11)^\times$, which has order 10. In fact, one can check that $[2] \in (\mathbb{Z}/11)^\times$ has order 10 and thus $(\mathbb{Z}/11)^\times = \langle [2] \rangle$.

The map ρ is uniquely determined by $\alpha := \rho(x)$ and we get one such map for each $\alpha \in \mathrm{Aut}(K)$ with $\alpha^5 = e$. There are exactly five possibilites: $\alpha(y) = y^j$ for $j \in \{1, 3, 4, 5, 9\}$. (These are the even powers of 2 modulo 11.)

Following HW 8, we may give a presentation for the semi-direct product of two cyclic groups. We get that G is isomorphic to one of the five groups

$$P_j := \langle x, y | x^5, y^{11}, xyx^{-1} = y^j \rangle,\ j \in \{1, 3, 4, 5, 9\}.$$

Unlike the previous example, it's much less clear which of these are isomorphic to each other. The group P_1 is abelian and the other four are not. In fact, $P_2 \cong P_j$ for each of $j = 2, \ldots, 5$. For example, let's show

$$P_4 \cong P_3.$$

To keep things straight, let us write

$$P_4 := \langle x, y | x^5, y^{11}, xyx^{-1} = y^4 \rangle$$

and

$$P_3 := \langle a, b | a^5, b^{11}, aba^{-1} = b^3 \rangle.$$

Using the UMP for presentations, we may define a homomorphism

$$\phi : P_4 \to P_3$$

by sending x to a^4 and y to b. This exists since $\phi(x)^5 = (a^4)^5 = e$, $\phi(y)^5 = (b^5) = e$ and

$$\begin{aligned}
\phi(x)\phi(y)\phi(x^{-1}) &= a^4 b a^{-4} = a^3(aba^{-1})a^{-3} \\
&= a^2(ab^3a^{-1})a^{-2} = a^2(aba^{-1})^3a^{-2} = a^2b^{3^2}a^{-2} \\
&= a(ab^{3^2}a^{-1})a^{-1} = a(aba^{-1})^{3^2}a^{-1} = ab^{3^3}a^{-1} \\
&= ab^{3^3}a^{-1} = b^{3^4} = b^{81} = b^4 = \phi(y^4).
\end{aligned}$$

Notice that to find such a homomorphism sending x to a^i and y to b we need to solve the equation $3^i \equiv 4 \pmod{11}$.

Similaly we define a homomorphism

$$\psi : P_3 \to P_4$$

by sending a to x^4 and b to y. This exists since $\psi(a)^5 = (x^4)^5 = e$, $\phi(b)^{11} = y^{11} = e$ and

$$\begin{aligned}\phi(a)\phi(b)\phi(a^{-1}) = x^4yx^{-4} = x^3(xyx^{-1})x^{-3} = x^3y^4x^{-3}\\ = \cdots = y^{4^4} = y^{256} = y^3 = \phi(y^3).\end{aligned}$$

Notice that to find such a homomorphism sending a to x^j and b to y we need to solve the equation $4^j \equiv 3 \pmod{11}$.

Both composition $\phi \circ \psi$ and $\psi \circ \phi$ are readily verified to be identity maps using the uniqueness statement of the UMP of the presentation and the fact that these maps act as the identity on the generators: $(\phi \circ \psi)(a) = \phi(x^4) = (a^4)^4 = a^{16} = a$ and $(\phi \circ \psi)(b) = \phi(y) = b$, respectively $(\psi \circ \phi)(x) = \psi(a^4) = (x^4)^4 = x^{16} = x$ and $(\psi \circ \phi)(y) = \psi(b) = y$.

In conclusion, there are two isomorphism classes of groups of order 55: $\mathbb{Z}/55$ and $\langle a, b | a^5, b^{11}, aba^{-1} = b^3 \rangle$.

October 29, 2018

Example. Let us classify the groups of order 75 into isomorphism classes.

We will use two facts deduced from Sylow theory.

Fact 1: Every group of order 75 has a unique subgroup of order 25 and it is normal.

By the Main Theorem of Sylow Theory, $|\operatorname{Syl}_5(G)|$ must both be congruent to 1 modulo 5 and divide 3, and so clearly $|\operatorname{Syl}_5(G)| = 1$. That is, G has exactly one subgroup of order 25 and hence, by Lemma 1.114, it must be normal.

Fact 2: If A is a group of order $2^5 \cdot 3 \cdot 5$, then all the subgroups of order 3 of A are conjugate.

This is a direct consequence of the Main Theorem of Sylow Theory, as the action of G on $\operatorname{Syl}_5(G)$ is transitive.

I claim there are precisely 3 groups of order 75 up to isomorphism.

First let us show that there are at least 3 such groups. We have the abelian groups

$$\mathbb{Z}/25 \times \mathbb{Z}/3 \text{ and } \mathbb{Z}/5 \times \mathbb{Z}/5 \times \mathbb{Z}/3$$

and these are not isomorhic to each other since one has an element of order 25 and the other does not.

We construct a non-abelian group of order 75 as follows. Let H be a group isomorphic to $\mathbb{Z}/5 \times \mathbb{Z}/5$. It is best to write H multiplicatively, and so let y and z in H

correspond to the column vectors $\begin{bmatrix}1\\0\end{bmatrix}$ $\begin{bmatrix}0\\1\end{bmatrix}$ of $\mathbb{Z}/5 \times \mathbb{Z}/5$ under the isomophism. The 2×2 matrix

$$M = \begin{bmatrix}0 & -1\\1 & -1\end{bmatrix}$$

with entries in $\mathbb{F}_5$ has order 3 since $M \neq I_2$ and $M^3 = I_2$. Under the identification of $\mathrm{Aut}(N)$ with $\mathrm{GL}_2(\mathbb{F}_5)$, M corresponds to the unique automorphism α of N such that $\alpha(y) = z$ and $\alpha(z) = y^{-1}z^{-1}$. Now let $K = \langle x \rangle$ by cyclic of order 3. Since $\alpha^3 = \mathrm{id}$, there is a unique homomorphism $\rho : K \to \mathrm{Aut}(H)$ sending x to α. The resulting semi-direct product $G := H \rtimes_\rho K$ has order 75 and is non-abelian since the action is non-trivial. It has the presentation

$$P = \langle x, y, z \mid x^3 = y^5 = z^5 = e, yz = zy, xyx^{-1} = z, xyx^{-1} = y^{-1}z^{-1} \rangle.$$

Let us now sketch a proof that the three groups constructed so far are the only three groups of order 75, up to isomorphism. Assume G is a group and $\#G = 75$. Fact 1 shows that G has a normal subgroup H of order 25. By Cauchy's Theorem, there is an element x of order 3 and we set $K = \langle x \rangle$. It follows that $H \cap H = \{e\}$ and $HK = G$, so that

$$G \cong H \rtimes_\rho K$$

for some action $\rho : K \to \mathrm{Aut}(H)$ of K on H via automorphisms. Since H is cyclic of order 3 generated by x, such an action uniquely determined by an element $\alpha \in \mathrm{Aut}(H)$ with $\alpha^3 = \mathrm{id}$. By a homework problem, we know that

$$H \cong \mathbb{Z}/25 \text{ or } H \cong \mathbb{Z}/5 \times \mathbb{Z}/5.$$

In the former case, $\#\mathrm{Aut}(H) = 25 - 5 = 20$. Since $3 \nmid 20$, the only such element α is the identity automorphism, so that the map ρ must be the trivial map and thus the action of H on N is the trivial one. We get

$$G \cong \mathbb{Z}/25 \times \mathbb{Z}/3$$

in this case.

In the latter case, $H \cong \mathbb{Z}/5 \times \mathbb{Z}/5$, and so $\mathrm{Aut}(H) \cong \mathrm{GL}_2(\mathbb{F}_5)$. The elements α of $\mathrm{Aut}(H)$ we seek correspond to a two-by-two matrices A with entries in $\mathbb{F}_5$ such that $A^3 = I_2$. One possibility is $A = I_2$, so that α is the idenity map. This would give the group

$$G = \mathbb{Z}/5 \times \mathbb{Z}/5 \times \mathbb{Z}/3.$$

Another possibility is that A is the matrix above, and we would get the group P.

By Fact 2, since $\#\mathrm{Aut}(H) = (25-1)(25-5) = 24 \cdot 20 = 2^5 \cdot 3 \cdot 5$, any two subgroups of order 3 of $\mathrm{Aut}(H)$ are conjugate. Thus, given any two elements $\alpha, \alpha' \in \mathrm{Aut}(N)$ of order 3, the associated homomorphisms $\rho, \rho' : K \to \mathrm{Aut}(H)$ have images that are conjugate. By a homework problem on HW 9, it follows that

$$H \rtimes_\rho K \cong H \rtimes_{\rho'} K.$$

We conclude that there are exactly three isomorphism classes of groups of order 75.

1.7.4 The Fundamental Theorem of Finitely Generated Abelian Groups

Definition 1.133. A group G is finitely generated provided that $G = \langle A \rangle$, where A is a finite set.

Remark 1.134. Any finite group is finitely generated (take $A = G$), but a finitely generated group need not be finite.

Example. The following are finitely generated, but not finite groups:

- $\mathbb{Z} \cong F(\{x\})$
- $F(\{x_1, \ldots, x_n\})$ the free group on n letters
- $\underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{r \text{ terms}} = \mathbb{Z}^r = \langle a_1, \ldots, a_r \mid a_i a_j = a_j a_i \rangle$ the free abelian group of rank r.

We present one final theorem in this section, without proving it for now.

Theorem 1.135 (FTFGAG – elementary divisor form)**.** *Let G be a finitely generated abelian group. Then there exist $r, s \geq 0$, prime integers $p_1 < \ldots < p_s$ and positive integers $a_i \geq 1$ such that:*

1. *$G \cong \mathbb{Z}^r \times Q_1 \times \cdots \times Q_s$ where $|Q_i| = p_i^{a_i}$ for all i.*
2. *For each index i, there is a partition $a_i = a_{i,1} + \cdots + a_{i,j_i}$ with each $a_{i,j} \geq 1$, such that $Q_i \cong (\mathbb{Z}/p_i^{a_{i1}}) \times \cdots \times (\mathbb{Z}/p_i^{a_{i,j_i}})$.*
3. *The r, p_i's, j_i's and $a_{i,j}$'s are uniquely determined by G.*

Example. For $G \cong \mathbb{Z}/3 \times Z/5 \times Z/5$ we have $Q_1 = \mathbb{Z}/3$, $Q_2 = \mathbb{Z}/5 \times Z/5$.

Definition 1.136. In Theorem 1.135, the $p_i^{a_{i,k}}$ are the *elementary divisors* of G, and the decomposition of G in parts (1–2) is called the *elementary divisor decomposition* of G. The decomposition in part (1) is also called a *primary decomposition.*

Remark 1.137. In Theorem 1.135 (1), each Q_i is isomorphic to the unique Sylow p_i-subgroup of G.

October 31, 2018

Theorem 1.138 (FTFGAG – invariant factor form)**.** *Let G be a finitely generated abelian group. Then:*

1. *$G \cong \mathbb{Z}^r \times (\mathbb{Z}/n_1) \times \cdots \times (\mathbb{Z}/n_s)$ for some $r \geq 0, s \geq 0$, and $n_i \geq 2$ for all i, satisfying $n_{i+1} \mid n_i$ for all i.*
2. *The integers $r, s, n_1, \ldots, n_s$ are uniquely determined by G.*

Definition 1.139. In Theorem 1.138, the number r is the *rank* of G, the numbers $n_1, \ldots, n_s$ are the *invariant factors* of G, and the decomposition of G in part (1) is the *invariant factor decomposition* of G.

Rather than prove the FTFGAG (we will prove it in Math 818 using the theory of modules over principal ideal domains), let us show the equivalence of the two forms of the theorem. For this we need the Chinese Remainder Theorem.

Theorem 1.140 (Chinese Remainder Theorem)**.** *Suppose $m = p_1^{e_1} \cdots p_l^{e_l}$ for distinct primes $p_1, \ldots, p_l$. Then there is an isomorphism*

$$\phi : \mathbb{Z}/m \xrightarrow{\cong} \mathbb{Z}/(p_1^{e_1}) \times \cdots \times \mathbb{Z}/(p_l^{e_l})$$

given by

$$\phi([j]_m) = ([j]_{{p_1}^{e_1}}, \cdots, [j]_{{p_l}^{e_l}})$$

where $[j]_b$ denote the class of an integer j in $\mathbb{Z}/b$.

Proof. Using the UMP for infinite cyclic groups, we let $\psi : \mathbb{Z} \to \mathbb{Z}/(p_1^{e_1}) \times \cdots \times \mathbb{Z}/(p_l^{e_l})$ be the unique homomorhism that sends 1 to $([1]_{{p_1}^{e_1}}, \cdots, [1]_{{p_l}^{e_l}})$. Then

$$\psi(j) = ([j]_{{p_1}^{e_1}}, \cdots, [j]_{{p_l}^{e_l}}).$$

Clearly $m \in \mathrm{Ker}(\psi)$ and so $\langle m \rangle \subseteq \mathrm{Ker}(\psi)$. Conversely, if $\psi(n) = 0$, then $p_i^{e_i} \mid n$ for all i and since $p_1^{e_1}, \ldots, p_l^{e_l}$ are pairwise relatively prime, it follows that $m \mid n$. This proves $\mathrm{Ker}(\psi) = \langle m \rangle$. By the UMP for quotient groups (Theorem 1.77), there is an induced injective homomorphism ϕ as in the statement. Finally, ϕ must also be onto for cardinality reasons. □

We could have also proved the above theorem in perhaps a more familiar way by using the First Isomorphism Theorem.

Equivalence of Theorem 1.135 and Theorem 1.138.

We will be a bit hand-wavey for this and give the idea through examples.

It suffices prove that for a given group G, we can recover its invariant factor form from its elementary divisor form, and vice versa.

Let's do a couple examples: Say I tell you

$$G \cong \mathbb{Z}^3 \times \mathbb{Z}/4 \times \mathbb{Z}/8 \times \mathbb{Z}/9 \times \mathbb{Z}/27 \times \mathbb{Z}/25$$

By CRT gives

$$\mathbb{Z}/8 \times \mathbb{Z}/27 \times \mathbb{Z}/25 \cong \mathbb{Z}/(8 \cdot 27 \cdot 25)$$

and

$$\mathbb{Z}/4 \times \mathbb{Z}/9 \cong \mathbb{Z}/(4 \cdot 9)$$

so that

$$G \cong \mathbb{Z}^3 \times \mathbb{Z}/(4 \cdot 9) \times \mathbb{Z}/(8 \cdot 27 \cdot 25).$$

Since $(4 \cdot 9) \mid (8 \cdot 27 \cdot 25)$, this is "in invariant factor form", and hence the rank of A is 3 and the invariant factors of A are $4 \cdot 9$ and $8 \cdot 27 \cdot 25$.

Suppose now I tell you

$$G \cong \mathbb{Z}^4 \times \mathbb{Z}/6 \times \mathbb{Z}/36 \times \mathbb{Z}/180.$$

Then by the Chinese Remainder Theorem

$$G \cong \mathbb{Z}^4 \times \mathbb{Z}/2 \times \mathbb{Z}/3 \times \mathbb{Z}/4 \times \mathbb{Z}/9 \times \mathbb{Z}/4 \times \mathbb{Z}/5 \times \mathbb{Z}/9,$$

given the elementary divisor form.

In general, given

$$G \cong \mathbb{Z}^r \times \mathbb{Z}/p_1^{e_1} \times \cdots \times \mathbb{Z}/p_l^{e_l}.$$

by applying the Chinese Remainder Theorem we have

$$G \cong \mathbb{Z}^r \times \mathbb{Z}/d_1 \times \cdots \times \mathbb{Z}/d_n$$

where d_n is the product of the elementary divisors of highest power for each *distinct* prime in the list $p_1, \ldots, p_l$, d_{n-1} is the product of the next highest possible prime powers, and so on.

Conversely, given

$$G \cong \mathbb{Z}^r \times \mathbb{Z}/d_1 \times \cdots \times \mathbb{Z}/d_n$$

with $d_1 \mid d_2 \mid \cdots \mid d_n$, we may apply the CRT to each $\mathbb{Z}/d_i$ to find its elementary divisor form. □

Chapter 2

Ring Theory

November 2, 2018

2.1 Introduction to rings

2.1.1 Definition and examples

Definition 2.1. A *ring* is a set R equipped with two binary operations, $+$ and $\cdot$, satisfying:

1. $(R, +)$ is an *abelian* group with identity element denoted 0,
2. $\cdot$ is associative (making $(R, \cdot)$ a semigroup)
3. $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$ hold for all $a, b, c \in R$.

R is a *unital ring* (or a *ring with identity*) if, in addition to (1), (2), (3)

(4) there is a multiplicative identity element written as 1 such that $1 \cdot a = a = a \cdot 1$ for all $a \in R$.

R is *commutative* if in addition to (1)–(3)

(5) $a \cdot b = b \cdot a$ holds for all $a, b \in R$.

R is a *division ring* if $1 \neq 0$, (1)–(4) and (6) hold

(6) $(R - \{0\})$ is a group under $\cdot$ (i.e. every $r \in (R - \{0\})$ has a multiplicative inverse)

R is a *field* if $1 \neq 0$ and (1)–(6) hold (i.e. a field is a commutative division ring).

Exercise 2.2. Commutativity of addition is a consequence of the other ring axioms.

Here are some basic consequences of the axioms.

Proposition 2.3 (Ring arithmetic)**.** *For any ring R and all $a, b \in R$ we have:*

1. $a \cdot 0 = 0 = 0 \cdot a$,

2. $(-a)b = -(ab) = a(-b)$,

3. $(-a)(-b) = ab$.

If moreover R is unital, then

4. 1 *is unique, and*

5. $(-1)a = -a$.

Example. 1. $R = \{0\}$ is called the *trivial ring*. Notice that in the trivial ring $0 = 1$. Conversely, if $1 = 0$ in a ring, then $R = \{0\}$, since in this case for all a, we have $a \cdot 0 = 0$ and hence $a = a \cdot 1 = a \cdot 0 = 0$.

2. $\mathbb{Z}$ is a commutative ring.

3. $\mathbb{Z}/n$ is a commutative ring under addition and multiplication modulo n. Note that $\mathbb{Z}/n$ is a field if any only if n is prime.

4. The familiar sets of "numbers" $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields.

5. (**Matrix ring**) If R is any ring (not necessarily commutative), so is $\mathrm{M}_n(R)$ for any natural number n, using the usual rules for addition and multiplication of square matrices.

6. (**The real Hamiltonian quaternion ring**) Let i, j, k be formal symbols and set $\mathbb{H}$ to be the four dimensional $\mathbb{R}$-vector space consisting of all expressions of the form $a + bi + cj + dk$ with $a, b, c, d \in \mathbb{R}$. Addition is vector space addition:

   $$(a+bi+cj+dk)+(a'+b'i+c'j+d'k) = (a+a')+(b+b')i+(c+c')j+(d+d')k.$$

   Multiplication is uniquely determined by the axioms of a ring together with the rules

   $$i^2 = j^2 = k^2 = -1, -ji = ij = k, -kj = jk = i, -ik = ki = j.$$

   and the fact that the real coefficients commute with each other and i, j, k.

   It's not obvious that the multiplication defined in this way satisfies associativity, but in fact it does (this amounts conditions very similar to the associativity of the group Q_8).

   $\mathbb{H}$ is a division ring, since one can check that

   $$(a + bi + cj + dk)^{-1} = \frac{a - bi - cj - dk}{\|a + bi + cj + dk\|}$$

   where

   $$\|a + bi + cj + dk\| := a^2 + b^2 + c^2 + d^2.$$

In the equation above $\|a+bi+cj+dk\|$ is non-zero real number if $a+bi+cj+dk$ is not the zero element. The quantity $\|a+bi+cj+dk\|$ is called the *norm* of the quaternion $a+bi+cj+dk$.

7. (**Direct product of rings**) The cartesian product $R \times R'$ of two rings R and R' has a natural ring structure with addition and multiplication defined componentwise:
$$(a,b)+(c,d) = (a+c, b+d)$$
$$(a,b)\cdot(c,d) = (a\cdot c, b\cdot d)$$

8. If X is a set and R is a ring, let $\mathrm{Fun}(X,R)$ be the collection of set theoretic functions from X to R, and define $(f+g)(x) = f(x)+g(x)$ and $(f\cdot g)(x) := f(x)\cdot g(x)$. Then $\mathrm{Fun}(X,R)$ is a ring. If X is a finite set and $|X| = n$, then $\mathrm{Fun}(X,R)$ may be identified with $R^n = \underbrace{R\times\cdots\times R}_{n}$, the direct product of n copies of R.

9. (**Endomorphism ring**) If $A = (A,+)$ is any abelian group, set $\mathrm{End}_{Ab}(A)$ to be the collection of endomorphisms of A — that is, the set of group homomorphisms $f : A \to A$ from A to itself.

   Then $\mathrm{End}_{Ab}(A)$ is a ring with addition $(f+g)(a) := f(a)+g(a)$ and multiplication $f\cdot g := f\circ g$. This is almost always a non-commutative ring.

November 5, 2018

Units, zero divisors, integral domains

Definition 2.4. An element a of a unital ring R with $1 \neq 0$ is called a *unit* there exists $b \in R$ such that$ab = 1$ and $ba = 1$. In case such b exists, it is unique, it is called the inverse of a and denoted by a^{-1}.

Definition 2.5. The set of units of a non-trivial unital ring R is denoted $R^\times$. This forms a group $(R^\times, \cdot)$ with respect to multiplication.

Example. $\mathcal{M}_n(F)^\times = \mathrm{GL}_n(F)$.

Definition 2.6. A *zero-divisor* in a ring R is an element $x \neq 0$ such that $xy = 0$ or $yx = 0$ for some $y \neq 0$.

Definition 2.7. A unital ring R is an *integral domain* (often shortened to *domain*) if $1 \neq 0$, R is commutative, and R has no zero divisors.

Lemma 2.8. *If a is a zero divisor in a ring R, then a is not a unit.*

Proof. Suppose that a is both a zero divisor and a unit. Then there exists $b \neq 0$ such that $ab = 0$ or $ba = 0$. Multiplying either of these equations by a^{-1} gives $b = 0$, a contradiction. □

Example.
- Every field is an integral domain (follows from the previous lemma).
- $\mathbb{Z}/n$ is an integral domain if and only if n is prime (in which case it happens to be a field too) or $n = 0$ (in which case $\mathbb{Z}/0 \cong \mathbb{Z}$).

Definition 2.9. An element a of a ring R is called *nilpotent* if $a^n = 0$ for some integer $ngeq1$.

Lemma 2.10. *If a is a nilpotent element in a unital ring R, then $1 - a$ is a unit.*

Proof. Exercise. □

Subrings

Definition 2.11. A subring of a ring R is a subset $S \subset R$ such that S is a ring under the operations of R.

Lemma 2.12. *A nonempty subset S of a ring R is a subring iff either one of the following hold:*

1. *S is a subgroup of R closed under multiplication.*
2. *S is closed under subtraction and multiplication.*

Proof. Exercise. □

Example.
- $\mathbb{Z}$ is a subring of $\mathbb{Q}$, which is a subring of $\mathbb{R}$, which is a subring of $\mathbb{C}$.
- $2\mathbb{Z}$ is a subring without 1 of the ring Z with 1.
- The set of continuous functions mapping $[0, 1] \to \mathbb{R}$ is a subring of $\mathrm{Fun}([0, 1], \mathbb{R})$, denoted $\mathcal{C}([0, 1])$.
- The set $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{C}$ called the ring of Gaussian integers.

Definition 2.13. The *center* of a ring R is the set

$$Z(R) = \{z \in R \mid zr = rz \text{ for all } r \in R\}.$$

Lemma 2.14. *The center $Z(R)$ is a subring of R.*

Lemma 2.15. *Let d be a squarefree integer (that is, the prime factorization of d has no repeated primes). Then the subset $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$ of $\mathbb{C}$ is a subring that is a field (called a quadratic field), and $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} | a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{Q}(\sqrt{d})$.*

Proof. Both $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Z}[\sqrt{d}]$ are closed under subtraction and multiplication, so they are subrings of $\mathbb{C}$.

The fact that $\mathbb{Q}(\sqrt{d})$ is a *subfield* follows since $\mathbb{Q}(\sqrt{d})$ is also closed under taking inverses. Indeed the inverse of $r + q\sqrt{d}$ (from $\mathbb{C}$) turns out to be

$$(r + q\sqrt{d})^{-1} = \frac{r - q\sqrt{d}}{r^2 - dq^2} \in \mathbb{Q}(\sqrt{d})$$

whenever $r + q\sqrt{d} \neq 0$. A slightly subtle point here is that the fraction above makes sense since $r^2 - dq^2 \neq 0$ provided r and q are not simultaneously 0. This is because, if $r^2 - dq^2 = 0$ then either $d = (r/q)^2$, which contradicts the assumption that d is squarefree, or $r = q = 0$, which contradicts the assumption $r + q\sqrt{d} \neq 0$. □

Exercise 2.16. If R is a ring and S is a subring of R, it can happen that

1. R is unital but S is not (e.g. $S = 2\mathbb{Z} \subset R = \mathbb{Z}$)
2. S is unital but R is not
3. both R and S are unital but $1_R \neq 1_S$

Find examples for each of these situations!

Exercise 2.17. Any subring of a commutative ring is a commutative ring.
Any unital subring of an integral domain is an integral domain.

November 7, 2018

2.1.2 Group rings and polynomial rings

Here is another general example of a ring which will be a major player in Math 901.

Definition 2.18. Let $G = (G, \cdot)$ be a group and let R be a commutative ring with $1 \neq 0$ (often R is taken to be a field). Let $R[G]$ be the collection of formal expressions of the form indicated below, where the $+$ operation is assumed to be commutative:

$$R[G] = \{r_1 g_1 + r_2 g_2 + \cdots + r_n g_n, n \geq 0, r_i \in R, g_i \in G\}.$$

Equivelently, a typical element of $R[G]$ can be written as $\sum_{g \in G} r_g g$, where $r_g \in R$ for all g and $r_g = 0$ for all but a finite number of g's.

We can make $R[G]$ into a ring by defining

$$(\sum_{g \in G} r_g g) + (\sum_{g \in G} s_g g) = \sum_{g \in G} (r_g + s_g) g$$

and

$$(\sum_{g\in G} r_g g)\cdot(\sum_{h\in G} s_h h) = \sum_{z\in G}\sum_{(g,h),gh=z} r_g s_h z.$$

With these definitions, $R[G]$ is a ring, called the *group ring of* G with coefficients in R. It is a unital ring with identity $1_R e_G$. If $R = F$ is a field then $F[G]$ is an F-vector space.

Remark 2.19. Our book writes $R[G]$ as RG, but the notation $R[G]$ is more standard.

Lemma 2.20. *If F is a field, $F[G]$ is an F-vector space and G is a basis, so that* $\dim_F(F[G]) = \#G$.

Example. Take $G = S_3$ and $R = \mathbb{R}$. Then $\mathbb{R}[S_3]$ is a six dimensional real vector space with basis $\{e, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}$. An element is any expression of the form

$$r_1 e + r_2(1\,2) + r_3(1\,3) + r_4(2\,3) + r_5(1\,2\,3) + r_6(1\,3\,2)$$

where $r_1, \ldots, r_6$ are real numbers. This ring has some zero divisors — for example

$$(e - (1\,2))(e + (1\,2)) = e - (1\,2) + (1\,2) - (1\,2)^2 = e - e = 0.$$

Here we are abusing notation a bit — for example, $-(1\,2)$ is really $(-1_R)(1\,2)$. In general, $1_R g$ is just written as g in $R[G]$ and $(-r)g$ is just written as $-rg$, since $(-r)g$ is the additive inverse of rg.

Exercise 2.21. Let R be any commutative ring and G a group. Show $R[G]$ is commutative if and only if G is abelian.

We identify G as a subset of $R[G]$ in the obvious way (by identifying $1_R g$ with g).

Proposition 2.22. *For any commutative ring R, the inclusion $i : G \hookrightarrow R[G]$ given by $i(g) = 1_R g$ lands in $R[G]^\times$ and induces a homomorphism of abelian groups $G \to R[G]^\times$.*

Proof. Note that $(1_R g)(1_R h) = 1_R(gh)$ by definition of multiplication in $R[G]$.

This gives that for any $g \in G$ we have

$$(1_R g)(1_R g^{-1}) = (1_R g^{-1})(1_R g) = 1_R e_G = 1_{R[G]},$$

thus $i(g)$ is a unit in $R[G]$ with inverse $i(g^{-1})$. This shows that $\mathrm{Im}(i) \subseteq R[G]^\times$.

The formula $(1_R g)(1_R h) = 1_R(gh)$ also gives that the map $g \mapsto 1_R g$ is group homomorphism. □

Example. Let $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ denote the group of quaterinons and $\mathbb{R}$ the field of real numbers, and let us consider the group ring $\mathbb{R}[Q_8]$. Actually, the notation here is not so good since $(-1)k$ is easily confused with $1(-k)$, and, even worse, things liks $1 \cdot 1$, $1 \cdot (-1)$ are highly confusing. So, let us rename the elements of Q, so that

$$Q_8 = \{e, e', i, i', j, j', k, k'\}$$

so that e is what we were writing as 1, e' is what we were writing as -1, i' is what we were writing as $-i$, etc. So, for example, we now have $i^2 = e'$ in this group.

$\mathbb{R}[Q_8]$ is a non-commutative ring, and you might guess that it is the same as the quaterinons $\mathbb{H}$ defined above, but it can't be: $\mathbb{R}[Q_8]$ is 8-dimensional as a $\mathbb{R}$-vector space whereas $\mathbb{H}$ is 4 dimensional. In fact $\mathbb{R}[Q_8]$ is not a division ring, since it has zero divisors: $(e-i)(e+i+i^2+i^3) = 0$ and so neither of the two factors can be units.

The problem is that $(-1)e \in R[Q_8]$ is *not* the same thing as $1e' \in R[Q]$, but we want them to be the same in $\mathbb{H}$. Once we learn about quotient rings, we will be able to show that $\mathbb{H}$ is the quotient of $R[Q_8]$ by the ideal generated by $e' + e$. Roughly this means we mod out by the relation $e' \sim -e$ and all consequences of this relation. For example, once one imposes this equivalence relation, the element

$$e + i + i^2 + i^3 = e + i + e' + e'i = (e + e') + i(e + e')$$

becomes the zero element.

Example. Group rings give lots of cool examples of rings, but we will now just focus on the boring case when G is a free abelian group (written with multiplicative notation) generated by $x_1, x_2, \ldots, x_n$. In this case an element of G may be written uniquely as $x_1^{e_1}, \ldots, x_n^{e_n}$ for $e_1, \ldots, e_n \in \mathbb{Z}$. For any commutative ring R a typical element of $R[G]$ is thus

$$\sum_{e_1,\ldots,e_n \in \mathbb{Z}} r_{e_1,\ldots,e_n} x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$$

This is a *Laurent polynomial* in the variables $x_1, \ldots, x_n$ with R-coefficients.

Say $n = 1$ and let $x = x_1$, so that $G = \langle x \rangle$. Then $ax^{-3} + bx^1 + c + dx^5$ with $a, b, c, d \in R$ is a representative example of an element of $R[G]$. Addition is by combining like powers of x. Multiplication is uniquely determined by the fact that it must satisfy the distributive law and $x^i x^j = x^{i+j}$ for $i, j \in \mathbb{Z}$.

It is clear that from the rules for $+$ and $\cdot$ that if we consider those elements with $e_i \geq 0$ for all i in a Laurent polynomial ring, we obtain a subring:

Definition 2.23. Let G be a free abelian groups with generators $x_1, \ldots, x_n$. For any commutative ring R, the *polynomial ring in* $x_1, \ldots, x_n$, written $R[x_1, \ldots, x_n]$, is the subring of $R[G]$ consisting of (finite) sums of the form

$$\sum_{e_1,\ldots,e_n \in \mathbb{Z}_{\geq 0}} r_{e_1,\ldots,e_n} x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}.$$

Example. If $n = 1$, letting $x = x_1$, then $R[x]$ consists of all expressions of the form $\sum_{i=0}^{\infty} r_i x^i$ with $r_i = 0$ for all but a finite number of i.

Definition 2.24. Let R be a commutative ring with $1 \neq 0$ and let M be a monoid (set endowed with a binary operation that is associative and has an identity). The *monoid*

ring $R[M]$ is the set of formal expressions

$$R[m] = \left\{ \sum_{m \in M} r_m m \mid r_m \in R, m \in, Mr_m = 0 \text{ for all but a finite number of } m \right\},$$

with operations defined by:

$$\left(\sum_{m \in M} r_m m \right) + \left(\sum_{m \in M} s_m m \right) = \sum_{m \in M} (r_m + s_m)\, m$$

$$\left(\sum_{m \in M} r_m m \right) \cdot \left(\sum_{m \in M} s_m m \right) = \sum_{mn=t} r_m s_n t.$$

Definition 2.25. The *polynomial ring* on n variables $x_1, \ldots, x_n$ with coefficients in R is the monoid ring $R[x_1, ..., x_n] = R(\mathbb{N}^n)$ on the free abelian monoid $\mathbb{N}^n$ where each x_i is identified with $(0, \ldots, 0, 1, 0, \ldots, 0)$ with the 1 in the i-th position.

Remark 2.26. When $R = \mathbb{R}$, one is tempted to think of $\mathbb{R}[x]$ as being a subring of the ring $\mathcal{C}(\mathbb{R})$ of continuous, real-valued functions that are defined on all of $\mathbb{R}$. This is not technically true: elements of $\mathbb{R}[x]$ are just formal expressions, not functions. But there is an injective ring homomorphism (see below)

$$\mathbb{R}[x] \hookrightarrow \mathcal{C}(\mathbb{R})$$

given by identifying a polynomial expression in one variable x having $\mathbb{R}$ coefficients with a function in the usual way.

November 9, 2018

2.1.3 Homomorphisms, ideals and quotient rings

Definition 2.27. If R and S are rings, a *ring homomorphism* from R to S is a function $f : R \to S$ that satisfies:

1. $f(x + y) = f(x) + f(y)$ for all $x, y \in R$,
2. $f(x \cdot y) = f(x) \cdot f(y)$ for all $x, y \in R$,

Lemma 2.28. *If $f : R \to S$ is a ring homomorphism then*

1. *$f(0_R) = 0_S$ and $f(-x) = -f(x)$.*
2. *if R, S are unital then $f(1_R)$ can be either $0_S, 1_S$ or a zero divisor.*
3. *If $f(1_R) = 1_S$ and $u \in R^\times$ then $f(u^{-1}) = f(u)^{-1}$.*

Proof. (2) Since $1_R 1_R = 1_R$ we have $f(1_R)f(1_R) = f(1_R)$, thus

$$f(1_R)(f(1_R) - 1_S) = 0_S.$$

Now either $f(1_R) = 0_S$ or $f(1_R) - 1_S = 0_S$ (which yields $f(1_R) = 1_S$) or both of these are nonzero and then they are complementary zero divisors (in particular, $f(1_R)$ is a zero divisor). □

Definition 2.29. A ring homomorphism $f : R \to S$ that is bijective is called a *ring isomorphism.*

A ring homomorphism $f : R \to S$ is a ring isomorphism if and only if the inverse function $f^{-1} : S \to R$ is also a ring homomorphism.

Definition 2.30. Two rings R and S are isomorphic, written $R \cong S$, if there is an isomorphism from R to S.

Lemma 2.31. *If $f : R \to S$ and $g : S \to T$ are ring homomorphisms (or isomorphisms, respectively), then $g \circ f : R \to T$ is a ring homomorphism (or isomorphism).*

Proposition 2.32. *The following are ring isomorphism invariants:*

1. *all group isomorphism invariants of the additive group, including the isomorphism class (i.e., if $R \cong S$ then $(R, +) \cong (S, +)$).*
2. *being unitary, commutative, division ring, field, integral domain*
3. *the number of zero divisors.*
4. *all group isomorphism invariants of the group of units, including the isomorphism class (i.e., if $R \cong S$ then $(R^\times, \cdot) \cong (S^\times, \cdot)$).*
5. *the isomorphism type of the center (i.e., if $R \cong S$ then $Z(R) \cong Z(S)$).*

Definition 2.33. For a ring R, an *ideal* (or a *two sided ideal*) of R is a non empty subset I such that

1. $(I, +)$ is a subgroup of $(R, +)$ and
2. for all $r \in R$ and $a \in I$, we have $ra \in I$ and $ar \in I$ (we can write this concisely as for all $r \in R$, $rI \subseteq I$ and $Ir \subseteq I$).

For non commutative rings, one speaks also about left ideals and right ideals. A *left ideal* is a subgroup of $(R, +)$ which satisfies for all $r \in R$ $rI = I$, while a *right ideal* is a subgroup of $(R, +)$ which satisfies and for all $r \in R$ $Ir = I$.

Example. • In any ring R, $\{0\}$ and R itself are ideals.

- The ideals of $\mathbb{Z}$ are $n\mathbb{Z}$. (These are all *principal* ideals so, $\mathbb{Z}$ is a PID – to be defined.)
- The sets $R_i = \left\{ \begin{bmatrix} 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ a_{i1} & a_{i2} & \cdots & a_{in} \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 \end{bmatrix} \right\}$ and $L_j = \left\{ \begin{bmatrix} 0 & \cdots & a_{j1} & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \\ 0 & \cdots & a_{ji} & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \\ 0 & \cdots & a_{jn} & \cdots & 0 \end{bmatrix} \right\}$ are a right ideal and a left ideal of $\mathrm{M}_n(R)$ respectively. Neither are two-sided ideals.

Remark 2.34. Any ideal I of a ring R is a subring of R, but not any subring is an ideal. For example, in $\mathbb{R}[x]$, the set S of polynomials for which every term has even degree is a subring (it's closed under subtraction and multiplication), but it is not an ideal because it is not closed under multiplication by arbitrary polynomials. Indeed, $p(x) = x^2 \in S$, but $xp(x) = x^3 \notin S$.

Exercise 2.35. An ideal I is *proper* if $I \neq R$. An ideal I of a unital ring R is proper if and only if I contains no units.

November 12, 2018

Here are some operations that one can perform with ideals.

Proposition 2.36. *Let R be a ring and let I, J be ideals of R. Then*

1. *$I + J := \{a + b \mid a \in I, b \in J\}$ is an ideal*
2. *$I \cap J$ is an ideal*
3. *$IJ = \{\sum_{i=1}^{n} a_i b_j \mid n \geq 0, a_i \in I, b_j \in J\}$ is an ideal and $IJ \subseteq I \cap J$.*
4. *The intersection $\bigcap_{\alpha \in J} I_\alpha$ of any collection of ideals I_α of R is an ideal.*

The set of all ideals of a ring R is a lattice with respect to the partial order given by containment. In this lattice the supremum of a pair of ideals I, J is $I + J$ and the infimum is $I \cap J$.

Definition 2.37. If A is any subset of a ring R, the *ideal generated by A*, denoted (A), is the intersection of all ideals of R that contain A:

$$(A) = \bigcap_{I \text{ ideal of } R, A \subseteq I} I.$$

Remark 2.38. By Proposition 2.36, (A) is an ideal and it is the smallest ideal of R that contains A.

Lemma 2.39. *For a subset A of a unitary ring R, the ideal generated by A is given by*

$$(A) = \left\{ \sum_{i=1}^{n} x_i a_i y_i \mid a_i \in A, x_i, y_i \in R \right\}.$$

If R is commutative and A is any subset, then there is a simpler formula

$$(A) = \left\{ \sum_{i=1}^{n} r_i a_i \mid n \geq 0, r_i \in R, a_i \in A \right\}.$$

Proof. Exercise. □

Example.

- In the commutative ring $\mathbb{Z}$, we have $(2,3) = (1) = \mathbb{Z}$. Indeed any element $n \in \mathbb{Z}$ can be written as $n = (-n)\cdot 2 + n \cdot 3 = n \cdot 1$. Note that $1 = \gcd(2,3)$.
- In the commutative ring $\mathbb{Z}$, we have $(2,4) = (2) = 2\mathbb{Z}$, the set of all even integers. Notice this shows that different sets can generate the same ideal. Also note that $2 = \gcd(2,4)$.
- In $\mathbb{Z}[x]$, we have $(2,x) = \{a + xp(x) \mid a \text{ is even}, p(x) \in \mathbb{Z}[x]\}$ and this ideal cannot be generated by a single element.

Definition 2.40. Let I be an ideal of a ring R. The ideal I is *principal* if $I = (a)$ for some $a \in R$, that is, I is generated by a set with a single element. I is *finitely generated* if $I = (A)$ for some finite subset A of R.

Example.

- every ideal of $\mathbb{Z}$ is principal with $I = (n)$ for some $n \in \mathbb{Z}$ ($\mathbb{Z}$ is a PID)
- for any field F, every ideal of $F[x]$ is principal ($F[x]$ is a PID)
- for any field F, every ideal in $F[x_1, \ldots, x_n]$ is finitely generated, but not necessarily principal. This is a consequence of a deep theorem called the Hilbert Basis Theorem, which you may see in Math 902.

Proposition 2.41. *If $f : R \to S$ is a ring homomorphism, then*

1. *the image of f is a subring of S and*
2. *the kernel of f is an ideal of R.*
3. *f is injective if and only if $\mathrm{Ker}(f) = \{0\}$.*
4. *if I is an ideal of R then $f(I)$ is an ideal of $f(R)$.*
5. *if J is an ideal of S then $f^{-1}(J)$ is an ideal of R.*

Proof. (2) Since f is a ring homomorphism, it is in particular a group homomorphism $(R,+) \to (S,+)$. We know the kernel of a group homomorphism is a subgroup, so $\mathrm{Ker}(f) \leq (S,+)$. All that remains to be shown is that for any $r \in R$ $r\,\mathrm{Ker}(f) \subseteq \mathrm{Ker}(f)$ and $\mathrm{Ker}(f)r \subseteq \mathrm{Ker}(f)$. Let $x \in \mathrm{Ker}(f)$; then $f(x) = 0$ and $f(rx) = f(r)f(x) = 0$, $f(xr) = f(x)f(r) = 0$ show $rx, xr \in \mathrm{Ker}(f)$. □

Proposition 2.41 shows that every kernel is a two-sided ideal; we'll show below that the converse is also true i.e. every two-sided ideal I is the kernel of a ring homomorphism $R \to R/I$.

You should think of a two-sided ideal as analogous to a normal subgroup of a group, for two related reasons: (1) they are the things that occur as kernels of homomorphisms (of rings/groups) and (2) they are the things you are allowed to mod out by.

Definition 2.42. An equivalence relation $\sim$ on a ring R is *compatible with addition and multiplication* if whenever $r, s, t \in R$ and $r \sim s$ then $r + t \sim s + t, rt \sim st$, and $tr \sim ts$.

Theorem 2.43. *Let I be a subring of a ring R. The following are equivalent:*

1. *I is an ideal of R.*
2. *The equivalence relation $\sim_I$ defined by $s \sim_I t$ if and only if $s - t \in I$ is compatible with addition and multiplication.*
3. *The quotient group R/I (under addition) is a ring with multiplication*

$$(r + I)(s + I) = rs + I$$

and the quotient map $\pi R \to R/I, \pi(r) = r + I$ is a ring homomorphism with $\mathrm{Ker}(\pi) = I$.

Proof. 1. $\Rightarrow$ 2. If $s \sim_I t$ then $s - t \in I$, so for any $r \in R$ we have $r(s - t) \in I$ and $(s - t)r \in I$, otherwise written as $rs \sim_I rt$ and $sr \sim_I tr$. Also, $s \sim_I t$ implies $s + r \sim_I t + r$ as $s - t = (s + r) - (t + r) \in I$.

2. $\Rightarrow$ 3. The main point is the well-definedness of the operations: Since the ideal I is a normal subgroup of $(R,+)$ the set of cosets R/I is a group under addition. The remaining point is the well definedness of the multiplication. If $r \sim_I r'$ and $s \sim_I s'$ we deduce by compatibility with multiplication that

$$r \sim_I r' \Rightarrow rs \sim_I r's$$
$$s \sim_I s' \Rightarrow r's \sim_I r's'$$

which by transitivity implies $rs \sim_I r's'$. By definition of the relation $\sim_I$ this gives $rs - r's' \in I$, which by way of our criteria for coset equality from Lemma 1.64 (translated into additive notation) allows to conclude $rs + I = r's' + I$

The ring axioms which involve multiplication are left to check as an exercise.

The quotient map is known to be an additive group homomorphism with $\text{Ker}(\pi) = I$ by Lemma 1.75. From the definition for multiplication in R/I we have

$$\pi(rs) = rs + I = (r + I)(s + I) = \pi(r)\pi(s)$$

which allows to conclude that π is a ring homomorphism.

3. $\Rightarrow$ 1. Since $(R/I, +)$ is a group we know that I is a (normal) subgroup of $(R, +)$. Furthermore, if $a \in I$ and $r \in R$ then $a + I = 0 + I$ and by the well-definedness of multiplication we have $ra + I = r0 + I = 0 + I$, so $ra \in I$ and $ar + I = 0r + I = 0 + I$, so $ar \in I$. □

November 14, 2018

Definition 2.44 (Quotient ring)**.** For a two-sided ideal I of R, the set of additive cosets modulo I is $R/I = \{r + I : r \in R\}$. This is an abelian group with respect to addition given by $(r+I)+(s+I) = (r+s)+I$. The *quotient ring* of R modulo I is the set R/I with addition defined as above and multiplication given by $(r + I) \cdot (s + I) = (rs) + I$.

Example. If $I = (n)$ is an ideal in the ring $\mathbb{Z}$, then the quotient ring $\mathbb{Z}/(n)$ is the familiar ring $\mathbb{Z}/n$.

Theorem 2.45 (Universal Mapping Propery for Quotient Rings)**.** *If $f : R \to S$ is a ring homomorphism and $I \subseteq R$ is an ideal such that $I \subseteq \text{Ker}(f)$, there exists a well defined ring homomorphism $\overline{f} : R/I \to S$ such that $\overline{f}(r + I) = f(r)$. Furthermore, if f is surjective then $\overline{f}$ is surjective and if $I = \text{Ker}(f)$ then $\overline{f}$ is injective.*

Proof. Ignoring $\cdot$ for a minute, we know that there is a unique homomorphism $\overline{f}$ of abelian groups from $(R/I, +)$ to $(S, +)$ such that $\overline{f}(r + I) = f(r)$. It remains only to check that $\overline{f}$ preserves multiplication: Given elements $r+I, s+I \in R/I$, their product is $rs + I$, and we have

$$\overline{f}(rs + I) = f(rs) = f(r)f(s) = f(r + I)f(s + I),$$

since f preserves multiplication. □

2.1.4 Isomorphism Theorems for rings

Theorem 2.46 (First Isomorphism Theorem for Rings)**.** *If $f : R \to S$ is a ring homomorphism, then $R/\text{Ker}(f) \cong \text{Im}(f)$ via the map $\overline{f}$ given by $\overline{f}(r+\text{Ker}(f)) = f(r)$.*

Proof. The map $\overline{f}$ is a well-defined ring homomorphism by the UMP for quotient rings. By the First Isomorphism Theorem for groups, the map $\overline{f}$ is bijective, finishing the proof. □

Exercise 2.47 (Evaluation homomorphism)**.** If $R \subseteq S$ are commutative rings with $1 \neq 0$ and $a \in S$, then the evaluation at a function $\phi : R[x] \to S$ given by $\phi(f(x)) = f(a)$ is a ring homomorphism.

The evaluation homomorphism is a particular case of the UMP for polynomial rings, which we will discuss later.

Example. Here is a nice application of the First Isomorphism Theorem. Consider the ring $\mathbb{R}[x]$ and let $I = (x^2+1)$ be the principal ideals generated by x^2+1. Since $\mathbb{R}[x]$ is commutative, we have

$$(x^2+1) = \{g(x)(x^2+1) \mid g(x) \in \mathbb{R}[x]\},$$

so (x^2+1) is simply the collection of polynomials having x^2+1 as a factor. I claim that $\mathbb{R}[x]/(x^2+1)$ is isomorphic as a ring to $\mathbb{C}$. To prove this we define a map

$$\phi : \mathbb{R}[x] \to \mathbb{C}$$

sending $f(x)$ to $f(i)$, the evaluation of f at i. It is easy to check ϕ is a ring homomorphism and it is onto since elements of the form $a+bx$ in the source map to all possible complex numbers under ϕ.

We claim the kernel of ϕ is (x^2+1). It is clear that $x^2+1 \in \text{Ker}(\phi)$ and it follows that $(x^2+1) \subseteq \text{Ker}(\phi)$, since $\text{Ker}(\phi)$ is a two-sided ideal. Suppose $\phi(f(x)) = 0$ and write $f(x) = (x^2+1)q(x) + r(x)$ with degree of $r(x)$ at most one, using the division algorithm in the polynomial ring $\mathbb{R}[x]$. So $r(x) = a + bx$ for real numbers a, b. If $r(x) \neq 0$, then $r(i) \neq 0$, which would contradict $f(i) = 0$. So we must have $r(x) = 0$ and hence $f(x) \in (x^2+1)$.

Applying the First Isomorphism Theorem for Rings, we get

$$\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$$

via the map sending $f(x) + (x^2+1)$ to $f(i)$.

Intuitively, we have adjoined a formal symbol x to the real numbers, and by modding out x^2+1 we have forced x to be a square root of -1. That is, we have adjoined i to the real numbers, obtaining $\mathbb{C}$.

Theorem 2.48 (Second Isomorphism Theorem for rings)**.** *Let S be a subring and let I be an ideal of R. Then $S + I = \{s + i \mid s \in S, i \in I\}$ is a subring of R, $S \cap I$ is an ideal of S, and*

$$\frac{S+I}{I} \cong \frac{S}{S \cap I}.$$

Theorem 2.49 (Third Isomorphism Theorem for rings)**.** *If R is a ring and $I \subseteq J$ are two ideals of R, then J/I is an ideal of R/I and*

$$\frac{R/I}{J/I} \cong R/J \text{ via } (r+I) + J/I \mapsto r + J.$$

November 16, 2018

Before we can show some examples related to the Third Isomorphism Theorem, we need to discuss the reduction homomorphism for polynomials.

Lemma 2.50 (Reduction homomorphism)**.** *Given a ring map $\phi : R \to S$ between commutative rings, there is an induced ring map*

$$\rho : R[x] \to S[x], \rho\left(\sum_i r_i x^i\right) = \sum_i \phi(r_i) x^i.$$

In particular, for I an ideal of R and $S = R/I$ this homomorphism maps $\sum_i r_i x^i \mapsto \sum_i \overline{r_i} x^i$ where $\overline{r_i}$ denotes the coset of each coefficient modulo I and $\mathrm{Ker}(\rho) = I$.

Proof. Exercise. □

In the following we'll use the reduction homomorphism $\rho : \mathbb{Z}[x] \to (\mathbb{Z}/2)[x]$. Since we denote congruence classes in $\mathbb{Z}/2$ by $[-]$, this homomorphism will be given by $\sum_i a_i x^i \mapsto \sum_i [a_i] x^i$ for $a_i \in \mathbb{Z}$.

Example. Consider the ideal $J = (2, x^2 + x + 1)$ of $\mathbb{Z}[x]$. Explicitly, by Lemma 2.39 we have

$$J = \{p(x) \cdot 2 + q(x)(x^2 + x + 1) \mid p(x), q(x) \in \mathbb{Z}[x]\}.$$

Suppose we want to understand $\mathbb{Z}[x]/J$. Then the Third Isomorphism Theorem is our friend. Set $I = (2)$ and note that $I \subseteq J$, and so by the Third Isomorphism Theorem

$$\mathbb{Z}[x]/J \cong \frac{\mathbb{Z}[x]/I}{J/I}.$$

Next we express both the numerator and the denominator in better terms. I claim

$$\mathbb{Z}[x]/I = \mathbb{Z}[x]/(2) \cong (\mathbb{Z}/2)[x].$$

To see this consider the reduction homomorphism $\rho : \mathbb{Z}[x] \to (\mathbb{Z}/2)[x]$ sending a polynomial $p(x)$ to its reduction modulo 2. The kernel of this surjective ring map is I, establishing our claim by the First Isomorphism Theorem.

Recall that J/I denotes the image of J under the quotient map $\pi : \mathbb{Z}[x] \to \mathbb{Z}[x]/I$. Therefore we have

$$\begin{aligned} J/I &= \pi(J) = \{\pi(p(x) \cdot 2 + q(x)(x^2 + x + 1)) \mid p(x), q(x) \in \mathbb{Z}[x]\} \\ &= \{\pi(p(x)) \cdot \pi(2) + \pi(q(x))\pi(x^2 + x + 1)) \mid p(x), q(x) \in \mathbb{Z}[x]\} \\ &= \{\pi(p(x)) \cdot 0 + \pi(q(x))\pi(x^2 + x + 1)) \mid p(x), q(x) \in \mathbb{Z}[x]\} \\ &= \{f(x)\pi(x^2 + x + 1)) \mid f(x) \in \mathbb{Z}[x]/I\} = ((x^2 + x + 1) + I)\,. \end{aligned}$$

In other words, J/I is the ideal generated by the coset of $x^2 + x + 1$ in $Z[x]/(2)$.

Moreover, under the isomorphism $\bar{\rho} : \mathbb{Z}[x]/I \to (\mathbb{Z}/2)[x]$ discussed above, we have that $f(x) + I \mapsto \overline{f}(x)$, where $\overline{f}(x)$ denotes the reduction of the coefficients of f modulo 2. Therefore $\bar{\rho}(J/I) = ([1]x^2 + [1]x + [1])$, where $[1]$ denotes the congruence class of 1 modulo 2.

Now we put everything together: consider the ring homomorphism $\varphi = \pi' \circ \bar{\rho}$ where

$$\mathbb{Z}[x]/I \xrightarrow{\bar{\rho}} (\mathbb{Z}/2)[x] \xrightarrow{\pi'} \frac{(\mathbb{Z}/2)[x]}{([1]x^2 + [1]x + [1])}.$$

Notice that since $\bar{\rho}$ and π' are surjective, so is φ, thus $\mathrm{Im}(\varphi) = \frac{(\mathbb{Z}/2)[x]}{([1]x^2+[1]x+[1])}$ and

$$\mathrm{Ker}(\varphi) = \mathrm{Ker}(\pi' \circ \bar{\rho}) = \mathrm{Ker}(\pi') = ([1]x^2 + [1]x + [1])$$

since $\bar{\rho}$ is an isomorphism and π' is a quotient map, Applying the First Isomorphism Theorem to φ gives

$$\frac{\mathbb{Z}[x]/I}{J/I} \cong \frac{(\mathbb{Z}/2)[x]}{([1]x^2 + [1]x + [1])}$$

and combining this with the Third Isomorphism Theorem further yields

$$\mathbb{Z}[x]/J \cong \frac{(\mathbb{Z}/2)[x]}{([1]x^2 + [1]x + [1])}.$$

As discussed before in Proposition 2.36, the set of all all ideals in a ring R is a partially ordered set with respect to the order given by containment.

Theorem 2.51 (Lattice Theorem for Quotient Rings)**.** *Suppose R is a ring and I is a two-sided ideal of R, and write $\pi : R \to R/I$ for the quotient ring homomorphism. There is a bijection*

$$\Psi : \{\textit{subrings of } R \textit{ containing } I\} \to \{\textit{subrings of } R/I\}, \Psi(S) = \pi(S) = S/I$$

with inverse

$$\Psi^{-1} : \{\textit{subrings of } R/I\} \to \{\textit{subrings of } R \textit{ containing } I\}, \Psi^{-1}(S) = \pi^{-1}(S).$$

Moreover this bijection induces a bijection between

$$\{\textit{ideals of } R \textit{ containing } I\} \leftrightarrow \{\textit{ideals of } R/I\}$$

since I is an ideal of R if and only if $\Psi(I)$ is an ideal of R/I.

Example. It turns out that the ring $F = \frac{(\mathbb{Z}/2)[x]}{([1]x^2+[1]x+[1])}$ we discussed in the previous example is a field and by a problem from HW 11, any field F has only two ideals (0) and F itself. This implies via the Lattice Isomorphism Theorem that there are only two ideals in $(\mathbb{Z}/2)[x]$ which contain $([1]x^2+[1]x+[1])$, namely $([1]x^2+[1]x+[1]) = \pi^{-1}(0)$ and $(\mathbb{Z}/2)[x] = \pi^{-1}(F)$.

November 19, 2018

2.1.5 Prime and maximal ideals in commutative rings

Definition 2.52. A *maximal ideal* of an arbitrary ring R is a *proper* ideal M such that the only ideals of R containing M are M and R.

A *prime ideal* of a commutative ring R is a *proper* ideal P such that whenever $xy \in P$ for $x, y \in R$, we have $x \in P$ or $y \in P$.

Exercise 2.53. An ideal P is prime if and only if $R \setminus P$ is closed under multiplication.

Example.
- In $\mathbb{Z}$, the prime ideals are (0) and the ideals generated by prime integers $P = (p)$, where p is a prime integer. The maximal ideals are the ideals generated by prime integers. In particular (0) is prime but not maximal.
- In $\mathbb{Z}[i]$ the ideal (13) is not prime, because $13 = (3 + 2i)(3 - 2i) \in (13)$, but $3 + 2i \notin (13)$ and $3 - 2i \notin (13)$ (because if $3 \pm 2i = 13\alpha$ then $N(3 \pm 2i) = N(13)N(\alpha)$ so $13 = 13^2 N(\alpha)$, a contradiction).
- In $\mathbb{Z}[x]$ the ideal $(2, x)$ is maximal and prime (proof in the example given later), the ideals (2) and (x) are prime but not maximal.

Exercise 2.54. If R is a domain, S is a ring and $f : R \to S$ is a ring homomorphism, then $\mathrm{Ker}(f)$ is a prime ideal.

Theorem 2.55. *Let R be a commutative ring with $1 \neq 0$, and let I be an ideal of R.*

1. *The ideal I is maximal if and only if R/I is a field.*
2. *The ideal I is prime if and only if R/I is an integral domain.*
3. *Every maximal ideal of R is prime.*

Proof.
1. The first assertion follows immediately from the Lattice Isomorphism Theorem and the fact that R/I is a field if and only if its only ideals are 0 and R/I.
2. Suppose I is prime. If $(r + I)(r' + I) = 0 + I$, then $rr' \in I$ and hence either $r \in I$ or $r' \in I$, so that either $r + I = 0$ or $r' + I = 0$. This proves R/I is a domain. Suppose R/I is a domain and that $xy \in I$. Then $(x + I)(y + I) = 0$ in R/I and hence either $x + I = 0$ or $y + I = 0$. It follows $x \in I$ or $y \in I$, so that I is prime.
3. If I is maximal, then R/I is a field, which in particular implies that R/I is a domain, so I is prime.

□

Example. We show that in $\mathbb{Z}[x]$ the ideal $(2, x)$ is maximal. For this we consider the quotient ring $\mathbb{Z}[x]/(2, x)$. By the Third Isomorphism Theorem, and because $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$ and under this isomorphism $(2, x)/(x)$ is mapped to (2), we have (ommitting some details)

$$\frac{\mathbb{Z}[x]}{(2, x)} \cong \frac{\mathbb{Z}[x]/(x)}{(2, x)/(x)} \cong \mathbb{Z}/2, \text{ a field.}$$

Since the quotient ring is field, we conclude that $(2, x)$ is maximal.

Axiom 2.56 (Zorn's Lemma)**.** *If $\mathcal{A}$ is a nonempty poset such that every totally ordered subset $\mathcal{B} \subseteq \mathcal{A}$ (that is, for all $b, b' \in \mathcal{B}$ either $b \leq b'$ or $b' \leq b$) has an upper bound in $\mathcal{A}$ (that is, there exists an element $u_B \in \mathcal{A}$ such that $b \leq u_{\mathcal{B}}$ for all $b \in \mathcal{B}$), then there is a maximal element $m \in \mathcal{A}$ (that is, there is an $m \in \mathcal{A}$ such that whenever $x \in \mathcal{A}$ and $m \leq x$ then $m = x$).*

November 26, 2018

Theorem 2.57. *If R is a ring with $1 \neq 0$ and I is a proper ideal of R, then there is a maximal ideal of R containing I. In particular there is a maximal ideal of R.*

Proof. Let $\mathcal{C}$ be the set of proper ideals of R that contain I and view $\mathcal{C}$ as a poset under containment. We will apply Zorn's Lemma. Suppose $\mathcal{T}$ is a totally ordered subset of $\mathcal{C}$. We need to show $\mathcal{T}$ has an upper bound in $\mathcal{C}$. If $\mathcal{T}$ is empty, I is such a bound. Otherwise, let $U = \bigcup_{L \in \mathcal{T}} L$.

- Since $\mathcal{T}$ is non-empty, we have $I \subseteq U$ and so $U \neq \emptyset$.
- Given $x, y \in U$, then $x \in L, y \in L'$ for some $L, L' \in \mathcal{T}$. Since $\mathcal{T}$ is totally ordered, either $L \subseteq L'$ or $L' \subseteq L$, and hence $x+y \in L$ or $x+y \in L'$. Either way, $x+y \in U$.
- For $x \in U$ and $r \in R$, we have $x \in L$ for some $L \in \mathcal{T}$ and hence $rx \in L \subseteq M$.

This proves U is an ideal that contains I. Since every $L \in \mathcal{T}$ is a proper ideal, $L \cap R^\times = \emptyset$, so $U \cap R^\times = \bigcup_{L \in \mathcal{T}} L \cap R^\times = \emptyset$ and hence U is a proper ideal, so $U \in \mathcal{C}$. By Zorn's Lemma, we conclude $\mathcal{C}$ has at least one maximal element M. This is a maximal ideal in the sense of definition 2.52 since if J is an ideal of R and $M \subseteq J$ then either $J = R$ or, if J is proper, then $J \in \mathcal{C}$, which yields $J = M$ by using that M is a maximal element of $\mathcal{C}$.

The existence of a maximal ideal follows by applying the first part of the thorem for $I = (0)$. □

2.1.6 Rings of fractions, a.k.a. localization

Next up we talk about the act of inverting elements in a commutative ring. To warm up, let's think about how one creates $\mathbb{Q}$ from $\mathbb{Z}$. An element of $\mathbb{Q}$ is a quotient of integers of the form $\frac{m}{n}$ with $m, n \in \mathbb{Z}$ and $n \neq 0$. But there is an equivalence relation, of course, because two such expressions $\frac{m}{n}$ and $\frac{m'}{n'}$ are deemed to be the same rational number iff $mn' = m'n$. Examining what makes this construction work leads to:

Definition 2.58. Suppose R is a commutative ring and $S \subseteq R$ is a subset such that

1. $1 \in S$,
2. S is closed under multiplication (i.e., if $x, y \in S$, then $xy \in S$), and
3. S does not contain 0 nor any zero divisors.

Such a subset S is called a *multiplicatively closed subset of nonzerodivisors* of R.

Example. Two types of multiplicatively closed sets are most commonly used in practice:

- If R is a domain and P is a prime ideal of R then $S = R \setminus P$ is a multiplicatively closed.
- If R is an arbitrary ring with $1 \neq 0$ and $x \in R$ is a non zero divisor then the set of non negative powers of x, $S = \{x^n \mid n \in \mathbb{Z}, n \geq 0\}$, is multiplicatively closed.

Definition 2.59. If R is a commutative ring and S is a multiplicatively closed subset of nonzerodivisors, the *ring of fractions* $S^{-1}R$ (also called the *localization* of R at S) is the set of equivalence clasees

$$S^{-1}R = \left\{ \frac{r}{s} \mid r \in R, s \in S \right\} / \sim$$

where the equivalence relation $\sim$ is defined by

$$\frac{r}{s} \sim \frac{r'}{s'} \text{ if and only if } rs' = r's.$$

From now on we just write $=$ instead of $\sim$ when dealing with fractions.
Addition and multiplication on $S^{-1}R$ are given by

$$\frac{r}{s} + \frac{r'}{s'} = \frac{rs' + r's}{ss'} \text{ and } \frac{r}{s} \cdot \frac{r'}{s'} = \frac{rr'}{ss'}.$$

Theorem 2.60. *If R is a commutative ring and S is a multiplicatively closed subset of nonzerodivisors, the rules given in the above definition for $+$ and $\cdot$ make $S^{-1}R$ into a commutative ring. Moreover, the function $R \to S^{-1}R$ sending r to $\frac{r}{1}$ is an injective ring homomorphism.*

Proof. There is a lot of small things to check and we'll just do a few. Right off the bat we need to be sure the given equivalence relation really is one. The relexive and symmatric properties are clear. But the proof of transitivity illustrates a key point: Say $\frac{r}{s} \sim \frac{r'}{s'} \sim \frac{r''}{s''}$. Then $rs' = r's$ and $r's'' = r''s'$. We need to deduce that $rs'' = r''s$. The given equations imply $rs's'' = r'ss'' = r''ss'$ and *since s' is a nonzerodivisor* we conclude $rs'' = r''s$. This is in fact the only time that the fact that S consists of nonzerodivisors is used.

We also need to be sure our rules for $+$ and $\cdot$ make sense and are independent of representation. They "make sense" since we assume S is closed under $\cdot$. To show $+$ is independent of representations, say $\frac{r}{s} \sim \frac{r''}{s''}$, so that $rs'' = r''s$. Then

$$\frac{r}{s} + \frac{r'}{s'} := \frac{rs' + r's}{ss'}$$

and

$$\frac{r''}{s''} + \frac{r'}{s'} := \frac{r''s' + r's''}{s''s'}$$

and so we need to show $(rs'+r's)(s''s') \sim (r''s'+r's'')(ss')$. This is clear upon expaning out both sides and using $rs'' = r''s$. In a similar way one shows $\cdot$ is well-defined.

From now on we just write $=$ instead of $\sim$ when dealing with fractions.

The associative and distributive axioms involve a straightfoward but tedious check, and we skip them entirely. The fact that $+$ and $\cdot$ are commutative is clear from their definitions. $S^{-1}R$ is a group under addition since it has a 0 element, namely $\frac{0}{1}$, and $\frac{r}{s} + \frac{-r}{s} = \frac{rs-rs}{s^2} = \frac{0}{s^2} = \frac{0}{1}$, with the last equality holding since $0 \cdot 1 = s^2 \cdot 0$. The 1 element is $\frac{1}{1}$. (Note that we have used that $1 \in S$ a couple times here — indeed, without this assumption S could be empty and then $S^{-1}R$ would be the empty set.)

The fact that $r \mapsto \frac{r}{1}$ is a ring homomorphism is straightforward to check. Its injective since $\frac{r}{1} = \frac{0}{1}$ implies $r = 0$. □

Remark 2.61. If S contains 1 and is closed under $\cdot$ but does contain some zero divisors, then a ring of fraction construction $S^{-1}R$ still exists; the only modification needed is in the definition for the equivalence relation: declare $\frac{r}{s} \sim \frac{r'}{s'}$ iff $s''(rs' - r's) = 0$ for some $s'' \in S$. In that case, the map $R \to S^{-1}R$ is no longer necessarily injective.

November 28, 2018

Corollary 2.62. *Let R be an integral domain and let $S = R \setminus \{0\}$. Then S is a multiplicatively closed subset of nonzerodivisors and $S^{-1}R$ is a field.*

Proof. R being a domain means $xy = 0$ implies ($x = 0$ or $y = 0$). The contrapositive to this statement is: if $x \neq 0$ and $y \neq 0$ then $xy \neq 0$, which shows S is a multiplicatively closed set of nonzerodivisors.

It remains only to show every non-zero element of $S^{-1}R$ is a unit. Given $\frac{r}{s} \neq 0$, note that $r \neq 0$ and hence $r \in S$. So $\frac{s}{r}$ is also an element of $S^{-1}R$. We have $\frac{r}{s}\frac{s}{r} = \frac{sr}{sr} = \frac{1}{1}$, where the last equation holds by the definition of $\sim$. □

Definition 2.63. If R is an integral domain and $S = R \setminus \{0\}$, the field $S^{-1}R$ is called the *field of fractions* of R. We denote this field of fractions by $\mathrm{Frac}(R)$.

Example.

- For a specific example, the field of fractions of $\mathbb{Z}$ is of course $\mathbb{Q}$.
- For another, if d is a squarefree integer and $R = \mathbb{Z}[\sqrt{d}]$ is an integral domain and we will show soon that its field of fractions is (isomorphic to) the field $\mathbb{Q}(\sqrt{d})$.
- For yet another, $\mathbb{R}[x]$ is an integral domain. Its field of fractions, usually denoted $\mathbb{R}(x)$ constists of all *rational functions*. This last example could be generalized by replacing $\mathbb{R}$ with any field and also by using any number of variables.

Theorem 2.64 (Universal Mapping Properity for rings of fractions)**.** *Let R be a commutative ring with $1 \neq 0$ and S a multiplicatively closed subset of nonzerodivisors such that $1 \in S$ and $0 \notin S$. If T is another commutative ring with $1 \neq 0$ and $\phi : R \to T$ is a ring homomorphism such that $\phi(s)$ is a unit of T for all $s \in S$, then there exists a unique ring homomorphism $\tilde{\phi} : S^{-1}R \to T$ such that $\tilde{\phi}(\frac{r}{1}) = \phi(r)$ for all $r \in R$. Moreover, $\tilde{\phi}(\frac{r}{s}) = \phi(r)\phi(s)^{-1}$.*

Proof. To show $\tilde{\phi}$ exists, note first of all that the formula

$$\tilde{\phi}\left(\frac{r}{s}\right) = \phi(r)\phi(s)^{-1},$$

is well-defined: if $\frac{r}{s} = \frac{r'}{s'}$ then $rs' = r's$ and so $\phi(r)\phi(s') = \phi(r')\phi(s)$. Since $\phi(s), \phi(s')$ are units we get $\phi(r)\phi(s)^{-1} = \phi(r')\phi(s')^{-1}$.

Checking that $\tilde{\phi}$ preserves $+$, $\cdot$ and 1's is now straightforward but tedious, and I omit the details.

For what comes next we need to establish the

Claim: $\phi(1_R) = 1_T$. By hypothesis, $\phi(1_R)$ is a unit in T. On the other hand, Lemma 2.28(2) shows that $\phi(1_R)$ can be either $0_T, 1_T$ or a zero divisor in T. Since units cannot be zero divisors, the only possiblity is $\phi(1_R) = 1_T$.

Let us now show that $\tilde{\phi}$ must satisfy the formula

$$\tilde{\phi}\left(\frac{r}{s}\right) = \phi(r)\phi(s)^{-1},$$

and hence is unique. We have by the definition of ring homomorphism that

$$\tilde{\phi}\left(\frac{r}{s}\right) = \tilde{\phi}\left(\frac{r}{1}\right)\tilde{\phi}\left(\frac{1}{s}\right) = \phi(r)\tilde{\phi}\left(\frac{1}{s}\right).$$

Also

$$\phi(s)\tilde{\phi}\left(\frac{1}{s}\right) = \tilde{\phi}\left(\frac{s}{1}\right)\tilde{\phi}\left(\frac{1}{s}\right) = \tilde{\phi}\left(\frac{s}{1}\cdot\frac{1}{s}\right) = \tilde{\phi}\left(\frac{1}{1}\right) = \phi(1_R) = 1_T.$$

Since $\phi(s)$ is a unit in S by assumption, this shows that

$$\tilde{\phi}\left(\frac{1}{s}\right) = \phi(s)^{-1}.$$

Combining this with the displayed equation above proves the desired formula.

□

Example. We show that for any squarefree integer d, $\mathrm{Frac}(\mathbb{Z}[\sqrt{d}]) \cong \mathbb{Q}(\sqrt{d})$.

Let ϕ be the inclusion map $\phi : \mathbb{Z}[\sqrt{d}] \hookrightarrow \mathbb{Q}(\sqrt{d})$. This extends by Theorem 2.64 to a ring homomorphism $\tilde{\phi} : \mathrm{Frac}(\mathbb{Z}[\sqrt{d}]) \to \mathbb{Q}(\sqrt{d})$ given by

$$\tilde{\phi}\left(\frac{\alpha}{\beta}\right) = \alpha\beta^{-1} \text{ for any } \alpha \in \mathbb{Z}[\sqrt{d}], \beta \in \mathbb{Z}[\sqrt{d}] \setminus \{0\}.$$

If $\tilde{\phi}\left(\frac{\alpha}{\beta}\right) = \tilde{\phi}\left(\frac{\gamma}{\delta}\right)$ then $\alpha\beta^{-1} = \gamma\delta^{-1}$ so $\alpha\delta = \beta\gamma$, which implies $\frac{\alpha}{\beta} = \frac{\gamma}{\delta}$, yielding that $\tilde{\phi}$ is injective. For any $\theta = \frac{m}{n} + \frac{i}{j}\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, we have $\theta = \frac{jm+ni\sqrt{d}}{nj} = \tilde{\phi}\left(\frac{jm+ni\sqrt{d}}{nj}\right)$, so $\theta \in \mathrm{Im}(\tilde{\phi})$ and so $\tilde{\phi}$ is a ring (actually, field) isomorphism.

2.1.7 The Chinese Remainder Theorem

Definition 2.65. Two ideals I, J of a ring R are *comaximal* if $I + J = R$.

Theorem 2.66 (Chinese Remainder Theorem)**.** *Let R be a commutative ring and let $I_1, \ldots, I_n$ be ideals. Then*

1. *The function*

$$h : R \to R/I_1 \times \cdots \times R/I_n \quad h(r) = (r + I_1, \cdots, r + I_n)$$

   is a ring homomophism with kernel $\mathrm{Ker}(h) = I_1 \cap \cdots \cap I_n$.

2. *If $I_1, \ldots, I_n$ are pairwise comaximal, then*

   - *h is surjective,*
   - $I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$
   - $R/I_1 \cdots I_n = R/I_1 \cap \cdots \cap I_n \cong R/I_1 \times \cdots \times R/I_n$

Proof. We prove the case $n = 2$ due to time constraints.

1. We only show how to compute the kernel

$$\begin{aligned}\mathrm{Ker}(h) &= \{r \in R \mid (r + 1_1, r + I_2) = (0 + I_1, 0 + I_2)\} \\ &= \{r \in R \mid r \in I_1 \text{ and } r \in I_2\} = I_1 \cap I_2.\end{aligned}$$

2. Assume that $I_1 + I_2 = R$ so that $a + b = 1$ for some $a \in I_1, b \in I_2$. To show $h : R \to R/I_1 \times R/I_2$ is onto, pick any $(x + I_1, y + I_2)$. Set $z = ay + bx$. Then

$$z + I_1 = bx + I_1 = (1 - a)x + I_1 = x + I_1$$

and

$$z + I_2 = ay + I_2 = (1 - b)y + I_2 = y + I_2.$$

So $h(z) = (x + I_1, y + I_2)$.

In general $I_1 I_2 = \{\sum_{i=0}^{n} a_i b_i \mid n \geq 0, a_i \in I_1, b_i \in I_2\} \subseteq I_1 \cap I_2$ holds for any pair of ideals. If $z \in I_1 \cap I_2$, then $z = z \cdot 1 = z(a + b) = za + zb \in I_1 I_2$.

The last statement follows by the First Isomorphism Theorem. □

November 30, 2018

2.2 "Nice" commutative rings: EDs, PIDs, UFDs

In this section we'll introduce the notions listed below and justify the containments.

$$\boxed{\text{Fields} \subset \text{Euclidean Domains} \subset \text{PIDs} \subset \text{UFDs} \subset \text{Integral domains}}$$

2.2.1 Euclidean domains (EDs)

We now introduce two related notions: Euclidean domain (ED) and principal ideal domain (PID).

Definition 2.67. A ring R is called a *principal ideal domain* (PID for short) if it is a domain with the property that every ideal is principal, i.e., for each ideal I, we have $I = (a)$ for some $a \in R$.

Examples of PIDs will come shortly.

A Euclidean domain is a domain with some additional structure, designed to mimic the parallel facts that in $\mathbb{Z}$ or $F[x]$, where F is a field, there is a notion of "division with remainder".

Definition 2.68. A *Euclidean domain* (ED) is a domain R together with a function $N : R \to \mathbb{Z}_{\geq 0}$ such that $N(0) = 0$ and the following property holds: for any two elements $a, b \in R$ with $b \neq 0$, there are elements q and r of R such that

$$a = qb + r \text{ and either } r = 0 \text{ or } N(r) < N(b).$$

One sometimes says that a Euclidean domain "has a division algorithm", but that's misleading: there need not be an algorithm to find q and r given a and b. Also, neither q nor r need be unique. Finally, I should mention that the function N is *not* required to satisfy any sort of multiplicative property, but in some examples it does and in those cases it is called a *norm function*.

Example. A "degenerate" example is a field F equipped with the trivial norm $N(r) = 0$ for all r. Given $a, b \in F$ with $b \neq 0$, we have $a = (ab^{-1})b + 0$.

This calculation shows, more generally, that if b is a unit, then for all a there exists an equation $a = bq + r$ with $r = 0$, not matter what norm N is used.

Example. The canonical example is, of course, $R = \mathbb{Z}$ with $N(m) := |m|$. This ring is a ED because of the familiar division theorem for integers.

Note that in this example there is no need to include "$r = 0$" in the description of the division algorithm, since $b \neq 0$ implies $|0| < |b|$. This is not the case in other examples. Also observe that as we've defined remainders they are *not* unique. For example, in dividing 13 by 5, both

$$13 = 2 \cdot 5 + 3 \text{ and } 13 = 3 \cdot 5 + (-2)$$

are considered valid.

One could make remainders (and hence quotients) unique for $\mathbb{Z}$ by insisting that remainders always be non-negative, but this is not part of the abstract theory since it doesn't generalize to all cases well.

Definition 2.69. Let R be a commutative ring with $1 \neq 0$. The *degree* of a nonzero polynomial $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$ with $a_n \neq 0$ is defined to be n. The 0 polynomial does not have a degree.

Proposition 2.70. *If R is a domain, then*

1. *$R[x]$ is a domain*
2. *for any nonzero polynomials $f, g \in R[x]$, $\deg(fg) = \deg(f) + \deg(g)$*
3. *the units of $R[x]$ are the units of R ($R[x]^\times = R^\times$)*

Proof. Exercise. □

Example. The next classical example is $R = F[x]$ with F a field and where we define the norm to be degree: $N(f(x)) = \deg(f(x))$ if $f \neq 0$ and $N(0) = 0$. This ring is a ED because of the familiar long division for polynomials.

Example. The ring $R = \mathbb{Z}[i]$ of Gaussian integers is a Euclidean domain with N being the usual complex (Euclidean) square norm $N(a + bi) = a^2 + b^2$. Let α, $\beta \in \mathbb{Z}[i]$ and let $\frac{\alpha}{\beta} = p + qi \in \mathbb{Q}(i)$ (here we use that the fraction field of $\mathbb{Z}[i]$ is $\mathbb{Q}(i)$). Now pick $s, t \in \mathbb{Z}$ so that $|p - s| \leq 1/2$ and $|q - t| \leq 1/2$. We have

$$\alpha = \beta(s + ti) + \beta(p + qi) - \beta(s + ti).$$

Set $q = s + ti$ and set $r = \beta(p + qi) - \beta(s + ti) = \beta(s + ti - (p + qi))$ and notice that $q \in \mathbb{Z}[i]$ because $s, t \in \mathbb{Z}$ and $r \in \mathbb{Z}[i]$ by closure. If $r = 0$ we're good, and if $r \neq 0$ then, using that the complex squared norm is multiplicative as well as the Pythagorean Theorem and the choice for s, t, we have

$$N(r) = N(\beta(s+ti-(p+qi))) = N(\beta)N(s+ti-(p+qi)) \leq N(\beta) \cdot (1/4+1/4) < N(\beta).$$

Thus the norm function N makes $\mathbb{Z}[i]$ into a Euclidean domain.

One of the main features of Euclidean domains is that they are examples of PIDs:

Proposition 2.71. *If R is a Euclidean domain, then R is a PID.*

Proof. Let N be the norm function making R into a Euclidean domain. Pick an ideal I. If I is the zero ideal, $I = (0)$. Otherwise pick a non-zero element b of I with $N(b)$ as small as possible. (Such a b exists by the well-ordering of $\mathbb{Z}_{\geq 0}$.) I claim $I = (b)$. It is clear that $(b) \subseteq I$. Pick $a \in I$. Then

$$a = bq + r$$

and either $r = 0$ or $N(r) < N(b)$. But note that $r = a - bq \in I$, and we cannot have both $r \neq 0$ and $N(r) < N(b)$ by our choice of b. So it must be that $r = 0$, and hence $a \in (b)$. □

December 3, 2018

2.2.2 Principal ideal domains (PIDs)

Example (A PID that is not a ED)**.** The ring $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right] = \left\{a + b\frac{1+\sqrt{-19}}{2} \mid a, b \in \mathbb{Z}\right\}$ is a PID, but not a Euclidean domain. It is the simplest example of such a ring, but the proofs of these claims are not easy. I will not cover a proof of this fact.

Definition 2.72. Let R be a domain. Two elements $r, s \in R$ are associates if there is a unit u of R such that $s = ur$.

Lemma 2.73. *Two elements x, y of a domain R are associates if and only if $(x) = (y)$.*

Proof. If $(x) = (y)$ then $x \in (y)$ and so $x = yu$ for some u. Similarly $y = xs$ and hence $y = yus$. Since R is a domain, either $y = 0$ or $su = 1$. If $y = 0$, then $x = 0 = 1y$ and otherwise u is a unit.

If $x = uy$ for a unit u, then $y = u^{-1}x$ and so $x \in (y)$ and $y \in (x)$, from which is follows that $(x) \subseteq (y)$ and $(y) \subseteq (x)$. □

Definition 2.74. Let R be a commutative ring and let $a, b \in R$.

- The element b is a *divisor* of a, and a is a multiple of b, written $b \mid a$ if there is an element $x \in R$ with $a = bx$.
- A *greatest common divisor*, or gcd, of a and b is an element $d \in R$ satisfying $d|a, d|b$, and whenever $d'|a$ and $d'|b$, then $d'|d$.
- A *least common multiple*, or lcm, of a and b is an element $m \in R$ satisfying $a|m, b|m$, and whenever $a|m'$ and $b|m'$ then $m|m'$.

Remark 2.75. Note that $b \mid a$ is equivalent to $b \in (a)$.

Proposition 2.76. *If R is a PID and $a, b \in R$, then*

1. *$(a, b) = (g)$ for some $g \in R$ and any such g is a gcd of a and b*
2. *the gcd of a and b is unique up to multiplication by a unit.*

Proof. 1. The existence of g is granted by definition in a PID. Now $a, b \in (g)$ gives that $g \mid a$ and $g \mid b$. If $g' \mid a$ and $g' \mid b$ we have that $a, b \in (g')$, so $(g) = (a, b) \subseteq (g')$ by minimality. This gives $g \in (g')$, hence $g' \mid g$. □

Remark 2.77. If R is not only a PID but a Euclidean domain with norm function N, then the Euclidean algorithm can be used to compute a gcd of any two nonzero $a, b \in R$.

Definition 2.78. Suppose R is a domain.

1. An element $p \in R$ is a *prime* element if $p \neq 0$ and the ideal (p) is a prime ideal.

2. An element $r \in R$ is *irreducible* if $r \neq 0$, r is not a unit, and whenever $r = xy$ with $x, y \in R$ then either x or y is a unit.

Example.
- the prime elements of $\mathbb{Z}$ are the prime integers and their negatives; they are also irreducible
- any element $\alpha \in Z[i]$ with $N(\alpha)$ a prime integer is irreducible e.g. $\alpha = 1 + 2i$ is irreducible
- the element $13 = (2 + 3i)(2 - 3i)$ is not irreducible in $\mathbb{Z}[i]$
- the polynomial $x^2 + x + [1] \in (\mathbb{Z}/2)[x]$ is irreducible; indeed if it factors non-trivially, it must factor as a product of two linear polynomials: $x^2 + x + [1] = (x + [a])(x + [b])$. Then $-[b]$ is a root for $x^2 + x + [1]$. But neither $[0]$ nor $[1]$ are roots for this polynomial, a contradiction.

Theorem 2.79. *Let R be a domain and let $r \in R$.*

1. *If r is a prime element, then r is irreducible.*

2. *If R is a PID and r is irreducible, then r is a prime element.*

Proof. Suppose R is an integral domain and that r is prime. Then $r \neq 0$ and r is not a unit. Suppose $r = yz$. Then $yz \in (r)$ and hence by definition either $y \in (r)$ or $z \in (r)$. If $y \in (r)$, we have $y = rt$ for some t and so $y = yzt$. Since $r \neq 0$, $y \neq 0$, and R is an integral domain, we must have $zt = 1$, showing that z is a unit.

Assume R is a PID and that r is irreducible. Since r is not a unit, (r) is a proper ideal and hence is contained in a maximal ideal M by Theorem 2.57. We show $(r) = M$ and hence (r) is prime. Since R is a PID, $M = (y)$ for some y. So $x = yt$ for some t. But x is irreducible and y is not a unit, which forces t to be a unit and hence $(x) = (y) = M$. □

Cutoff for final

December 7, 2018

2.2.3 Unique factorization domains (UFDs)

We now define UFD's.

Definition 2.80. A ring R is called a *unique factorization domain*, or *UFD* for short, if R is an integral domain and every element $r \in R$ that is non-zero and not a unit can be written as a finite product

$$r = p_1 \cdots p_n$$

of (not necessarily distinct) irreducible elements $p_1, \ldots, p_n$ of R in a way that is unique up to ordering and associates. That is, if

$$r = q_1 \cdots q_m$$

also holds with each q_i irreducuble, then $m = n$ and there is a permutation σ such that, for all i, we have p_i and $q_{\sigma(i)}$ are associates.

Example.

- $\mathbb{Z}$ is a UFD by the Fundamental Theorem of Arithmetic.
- $F[x]$ where F is a field is a UFD. This is the case because $F[x]$ is a Euclidean domain and Euclidean domains are UFD's (we'll prove this shortly).
- We will eventually prove that if R is a UFD then so is $R[x]$. It follows that $F[x_1, \ldots, x_n]$ is a UFD for all n. Note that if $n > 1$, this ring is not a PID and hence not a Euclidean domain.

Example (A UFD that is not a PID)**.** $\mathbb{Z}[x]$ is not a PID hence also not a Euclidean domain. For example, this can be seen because the ideal $(2, x)$ is not a principal ideal. It is a UFD because $\mathbb{Z}$ is a UFD (based on the result that if R is a UFD then so is $R[x]$ which we will prove shortly).

Example (A domain that is not a UFD)**.** $\mathbb{Z}[\sqrt{-5}]$ is a domain that is *not* a UFD, as $6 = (1+\sqrt{-5})(1-\sqrt{-5}) = 2 \cdot 3$ and each of $1+\sqrt{-5}, 1-\sqrt{-5}, 2, 3$ are irreducible by a norm argument (exercise).

Notice also that $\mathbb{Z}[\sqrt{-5}]$ contains elements that are irreducible but not prime: 2 is irreducible, by a norm argument. But it is not prime since $(1+\sqrt{-5})(1-\sqrt{-5}) \in (2)$ but neither $1+\sqrt{-5}$ nor $1-\sqrt{-5}$ is in (2).

We end the discussion by justifying the third containment in the chain

$$\boxed{\text{Fields} \subset \text{Euclidean Domains} \subset \text{PID's} \subset \text{UFD's} \subset \text{Integral domains}}$$

Theorem 2.81. *If R is a PID then R is a UFD.*

Proof. A sketch of the proof is the following:

- R a PID $\overset{2.83}{\Longrightarrow}$ R is Noetherian $\overset{2.84}{\Longrightarrow}$ existence of finite irreducible factorizations.
- R a PID$\overset{2.79}{\Longrightarrow}$ irreducible and prime elements coincide $\Longrightarrow$ uniqueness of irreducible factorizations.

□

The proof of the Theorem involves some intermediate results that are interesting in their own right.

Definition 2.82. Suppose R is a commutative ring. Then R is called a *Noetherian ring* if R satisfies the *ascending chain condition on ideals* — i.e., for every chain of ideals of R

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

there exists a positive integer n such that $I_n = I_{n+1} = I_{n+2} = \cdots = I_{n+k}$ for all $k \geq 0$.

Lemma 2.83. *If R is a PID then R is Noetherian.*

Proof. Consider and ascending chain of ideals of R; it must have the form

$$(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \cdots \subseteq (a_i) \subseteq (a_{i+1}) \subseteq \cdots .$$

Consider $I = \bigcup_{i \geq 1}(a_i)$ which is an ideal of R by the argument given in Theorem 2.57. Since R is a PID, $I = (b)$ for some $b \in R$. Since $b \in I = \bigcup_{i \geq 1}(a_i)$, we must have $b \in (a_n)$ for some n. Then we see that $I = (b) \subseteq (a_n) \subseteq (a_{n+1}) \subseteq \cdots (a_j) \subseteq \cdots \subseteq I$ for all $j \geq n$, thus $I = (a_j)$ for $j \geq n$ and the chain stabilizes as desired. □

Lemma 2.84. *If R is a Noetherian, integral domain, then every non-zero, not-unit element factors into a finite product of irreducible elements.*

Proof. Pick $x \in R$ with $x \neq 0$ and $x \notin R^\times$. If x is irreducible, there is nothing to prove. Otherwise, we have $x = x_1 x_2$ for non-units x_1, x_2. If both x_1, x_2 are irreducible, the proof is complete. Otherwise, one or both of them factors non-trivially. We may express this conveniently by saying that $x_1 = x_3 x_4$ and $x_2 = x_5 x_6$ such that either x_3 and x_4 are both non-units or x_5 and x_6 are both non-units. (E.g., if x_2 is irreducbile, we could set $x_5 = x_2, x_6 = 1$.) Continuing in the this manner, we form a binary tree with x at the top, x_1, x_2 one level down, x_3, x_4, x_5, x_6 one level below that, etc. We halt the process of building the tree if at some stage all the leaves of the tree are irreducbile elements, at which point we will have proven that x factors in to a product of the irreducible elements given by these leaves.

We need to rule out the possiblity that the process never terminates. If it never terminates, we will have built an infinite binary tree with the property that some route downward through the tree consists of an infinite list of of irreducible elements $y_1, y_2, y_3, \ldots$ such that $x = y_1 z_1$ for a non-unit z_1 and, for each $i \geq 1$, $y_i = y_{i+1} z_{i+1}$ for a non-unit z_{i+1}. Since R is an integral domain, we have $(x) \subsetneq (y_1)$ and $(y_i) \subsetneq (y_{i+1})$ for all $i \geq 1$. (E.g., if $(x) = (y_1)$ then $y_1 = xv$ and hence $x = xvz_1$, so that $vz_1 = 1$, contrary to z_1 being a non-unit.) But then we have arrived at an infinite ascending chain of ideals in R,

$$(x) \subsetneq (y_1) \subsetneq (y_2) \subsetneq (y_3) \subsetneq \cdots ,$$

which is not possible in a Noetherian ring. □

This completes the proof of existence of irreducible factorizations in PIDs according to the sketch of the proof of Theorem 2.81. Next we show the uniqueness statement, which follows from the next theorem:

Theorem 2.85. *Assume R is a Noetherian, integral domain having the property that every irreducible element is a prime element. Then R is a UFD.*

Proof. Since R is Noetherian, every element has a finite irreducible factorization by the previous Lemma.

Assume $x = p_1 \cdots p_n = q_1 \cdots q_m$ are two different irreducible factorization of x. Without loss, assume $n \leq m$. We induct on m. If $m = 1$ there is nothing to prove. Assume $m > 1$. Since we are assuming that irreducible elemnents are prime and p_n divides $q_1 \cdots q_m$, we have that p_n divides q_i for some i. Upon reordering, we may as well assume $q_m = p_n u$ for some u. Since q_m is also irreducible, u must be a unit. We get

$$p_1 \cdots p_n = q_1 \cdots q_{m-1} u p_n$$

and hence, since R is an integral domain, we may divide by p_n to obtatin

$$p_1 \cdots p_{n-1} = q_1 \cdots q_{m-2}(q_{m-1}u).$$

We are now done by induction. □

Math 818

January 7, 2019

2.3 Polynomial rings

Definition 2.86. For any commutative ring R, the *polynomial ring in the variable* x written $R[x]$ is the set

$$R[x] = \{a_n x^n + \ldots + a_1 x + a_0 \mid n \in \mathbb{Z}, n \geq 0, a_i \in R\}$$

with addition defined by

$$(a_n x^n + \ldots + a_1 x + a_0) + (b_n x^n + \ldots + b_1 x + b_0) = (a_n + b_n)x^n + \ldots + (a_1 + b_1)x + (a_0 + b_0)$$

and multiplication defined by

$$(a_n x^n + \ldots + a_1 x + a_0)(b_m x^n + \ldots + b_1 x + b_0) = \sum_{k=0}^{n+m} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) x^i.$$

Definition 2.87. For any commutative ring R, the *polynomial ring in* $x_1, \ldots, x_n$, written $R[x_1, \ldots, x_n]$, is defined inductively as $R[x_1, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x_n]$, but more easily thought of as the set consisting of (finite) sums of the form

$$R[x_1, \ldots, x_n] = \left\{ \sum_{e_1, \ldots, e_n \in \mathbb{Z}_{\geq 0}} r_{e_1, \ldots, e_n} x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n} \right\}$$

with addition and multiplication defined by rules similar to the ones in the previous definition.

Remark 2.88. One often views R as the subring of $R[x_1, \ldots, x_n]$ consisting of the constant polynomials.

Remark 2.89. Another way to define the polynomial ring $R[x_1, \ldots, x_n]$ is as the "free R-algebra generated by $x_1, \ldots, x_n$". This means that it is the smallest commutative ring containing R and $x_1, \ldots, x_n$ in which there are no relations involving the variables $x_1, \ldots, x_n$.

Definition 2.90. The degree of a nonzero polynomial $f = \sum_{e_1, \ldots, e_n \in \mathbb{Z}_{\geq 0}} r_{e_1, \ldots, e_n} x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$ is

$$\deg(f) = \max\{e_1 + \cdots + e_n \mid r_{e_1, \ldots, e_n} \neq 0\}.$$

The following facts about degree arithmetic are a generalization of Proposition 2.70.

Lemma 2.91. *Assume R is an integral domain.*

1. *$R[x_1, \ldots, x_n]$ is also an integral domain, for all $n \geq 1$.*
2. *$\deg(fg) = \deg(f) + \deg(g)$ if f and g are nonzero polynomials of $R[x_1, \ldots, x_n]$.*
3. *The units of $R[x_1, \ldots, x_n]$ are $R[x_1, \ldots, x_n]^\times = R^\times$ (the invertible constants).*

We have used the evaluation homomorphism in the past to build ring homomorphisms. Now we prove that this map is a homomorphism rigorously.

Proposition 2.92 (Universal mapping property for polynomial rings)**.** *Let R and S be commutative rings, $\phi : R \to S$ is a ring homomorphism and $s_1, \ldots, s_n$ arbitrary elements of S. Then there exists a unique ring homomorphism*

$$\tilde{\phi} : R[x_1, \ldots, x_n] \to S$$

such that $\tilde{\phi}|_R = \phi$ and $\tilde{\phi}(x_i) = s_i$ for all i, namely

$$\tilde{\phi}\left(\sum_{e_1,\ldots,e_n \geq 0} r_{e_1,\ldots,e_n} x_1^{e_1} \cdots x_n^{e_n}\right) = \sum_{e_1,\ldots,e_n \geq 0} \phi(r_{e_1,\ldots,e_n}) s_1^{e_1} \cdots s_n^{e_n}$$

Proof. Let's observe first that if such a map exists it is unique. For if $\tilde{\phi} : R[x_1, \ldots, x_n] \to S$ is a ring map extending ϕ and sending x_i to s_i. Then

$$\begin{aligned}\tilde{\phi}(\sum_{e_1,\ldots,e_n \geq 0} r_{e_1,\ldots,e_n} x_1^{e_1} \cdots x_n^{e_n}) &= \sum_{e_1,\ldots,e_n \geq 0} \psi(r_{e_1,\ldots,e_n}) \psi(x_1)^{e_1} \cdots \psi(x_n)^{e_n}) \\ &= \sum_{e_1,\ldots,e_n \geq 0} \psi(r_{e_1,\ldots,e_n}) s_1^{e_1} \cdots s_n^{e_n},\end{aligned}$$

using that $\tilde{\phi}$ preserves $+$ and $\cdot$.

For existence, let's assume $n = 1$ at first. Given $\phi : R \to S$ and $s \in S$, define

$$\tilde{\phi} : R[x] \to S$$

by

$$\tilde{\phi}(\sum_i r_i x^i) = \sum_i \phi(r_i) s^i.$$

It is elementary (but tedious) to check $\tilde{\phi}$ really is a ring homomorphism. The fact that it restricts to ϕ is clear, however.

For the general case, we proceed by induction on the number of variables n. The induction hypothesis shows that there is a ring homomorphism

$$\psi : R[x_1, \ldots, x_{n-1}] \to S$$

such that $\psi|_R = \phi$ and $\psi(x_i) = s_i$, $i = 1, \ldots, n-1$. Applying the $n = 1$ case to ψ gives

$$\tilde{\psi} : (R[x_1, \ldots, x_{n-1}])[x_n] \to S$$

with $\tilde{\psi}|_{R[x_1,\ldots,x_{n-1}]} = \psi$ and $\tilde{\psi}(x_n) = s_n$. Setting $\tilde{\phi} = \tilde{\psi}$ gives a map $\tilde{\phi}$ with the needed properties. □

A few special cases of the UMP for polynomial rings listed below are especially important as they arise often in practice.

Example (The evaluation homomorphism)**.** Suppose the ring map ϕ is the inclusion of a subring R into a commutative ring S, including even the case $R = S$. Given $s_1, \ldots, s_n \in S$. Then the map

$$\tilde{\phi} : R[x_1, \ldots, x_n] \to S$$

can be thought of as evaluation of polynomials in $x_1, \ldots, x_n$ at $s_1, \ldots, s_n$.

Example (Applying a ring homomorphism to the coefficients)**.** Given a ring map $\phi : R \to S$ between commutative rings, we may apply the Proposition to the composition $R \xrightarrow{\phi} S \hookrightarrow S[x]$ using the element $s = x$ of $S[x]$ to get an induced ring map

$$\tilde{\phi} : R[x] \to S[x]$$

that sends $\sum_i r_i x^i$ to $\sum_i \phi(r_i) x^i$. That is, the map $\tilde{\phi}$ applies ϕ to the coefficients of a polynomial. This can be generalized to more than one variable in the obvious way.

Example (The reduction homomorphism)**.** Continuing with the previous example, we could have $S = R/I$ for an ideal I of R and ϕ could be the quotient map. Then

$$\tilde{\phi} : R[x_1, \ldots, x_n] \to (R/I)[x_1, \ldots, x_n]$$

takes a polynomial and "reduces" its coefficients modulo I. We will usually denote the image of $f(x)$ through the reduction homomorphism by $\overline{f}(x)$.

January 9 2019

2.3.1 Polynomial rings that are UFD's

In this section we'll use two properties of UFD's that we list without proof:

- In a UFD a nonzero element is prime if and only if it is irreducible (this is similar to the PID case – compare with Theorem 2.79).
- Recall the definition of the greatest common divisor in Definition 2.74. In a UFD, for any two nonzero elements a gcd exists and can be computed as follows: if

  $$a = u p_1^{e_1} \ldots p_n^{e_n} \quad \text{and} \quad b = v p_1^{f_1} \ldots p_n^{f_n}$$

  are irreducible factorizations with u, v units and p_i irreducibles and $e_i, f_i \geq 0$ are integers then

  $$d = p_1^{\min\{e_1, f_1\}} \ldots p_n^{\min\{e_n, f_n\}} \text{ is a gcd for } a, b.$$

  More generally, for any collection of nonzero elements of a UDF with irreducible factorizations $a_i = u_i p_1^{e_{1i}} \ldots p_n^{e_{1n}}, 1 \leq i \leq m$, the following element is a gcd

  $$d = p_1^{\min\{e_{11}, \ldots, e_{1m}\}} \ldots p_n^{\min\{e_{n1}, \ldots, e_{nm}\}}.$$

The main goal of this section is to prove that, if R is a UFD then $R[x_1, \ldots, x_n]$ is a UFD as well. Thinking about the $n = 1$ case, the rough plan is to use the containment $R[x] \hookrightarrow F[x]$ where F is the field of fractions of R, exploiting the fact that $F[x]$ is a Euclidean domain and thus a UFD. In order to be able to pull back irreducible factorizations from $F[x]$ to $R[x]$ we need to know how irreducible elements are related among the two rings.

Theorem 2.93. *Let R be a UFD with field of fractions F. Regard R as a subring of F and view elements in $R[x]$ as also being elements of $F[x]$ via the induced map $R[x] \hookrightarrow F[x]$.*

1. **[Gauss's lemma]** *If $f(x) \in R[x]$ is irreducible in $R[x]$, then $f(x)$ remains irreducible as an element of $F[x]$.*

2. *If $f(x) \in R[x]$ is irreducible in $F[x]$ and the* gcd *of the coefficients of $f(x)$ is a unit, then $f(x)$ remains irreducible as an element of $R[x]$.*

Let me point out that this result is at least a tiny bit surprising.

Note that there are many irreducible polynomials in $\mathbb{R}[x]$ that do *not* remain irreducible in the larger ring $\mathbb{C}[x]$, e.g. $x^2 + 1$. So, in general, one might think that passing to a larger ring of coefficients would cause some irreducible polynomial to become reducible. Gauss' Lemma says that this is *not* the case if the larger ring is the field of fractions of the smaller one, provided the smaller one is a UFD.

Note also that the second statement is false if the gcd of the coefficients of f is not a unit. To see this, note that $2x + 6$ is irreducible in $\mathbb{Q}[x]$ but not in $\mathbb{Z}[x]$, since it factors as $2(x + 3)$. In $\mathbb{Q}[x]$, however, this factorization is trivial because 2 is a unit.

Proof of Theorem 2.93. 1. We will prove the contrapositive: if $f(x) \in R[x]$ is reducible in $F[x]$, then it is also reducible in $R[x]$. Say $f(x)$ factors nontrivially as $f(x) = A(x)B(x)$ in $F[x]$. Since F is a field, the units of $F[x]$ are the non-zero constant polynomials, and so having a nontrivial factorization means $\deg(A(x)), \deg(B(x)) > 0$. Each coefficient of A and B is a fraction, and so it is clear we can find a non-zero $d \in R$ such that $df(x) = a(x)b(x)$ where $a(x), b(x) \in R[x]$ have positive degree.

If d is a unit in R, then

$$f(x) = (d^{-1}a(x))b(x)$$

is a non-trivial factorization in $R[x]$ (since $R[x]^\times = R^\times$).

If d is not a unit, let $d = p_1 \cdots p_m$, $m \geq 1$, be an irreducible factorization of d. Since p_1 is irreducbile and R is a UFD, it is a prime element. We thus mod out by p_1 to get an equation

$$0 \cdot \overline{p}(x) = \overline{a}(x)\overline{b}(x)$$

in $(R/(p_1))[x]$ (where overlines denote applying the canonical map $R \twoheadrightarrow R/p_1$ to the coefficient of a poylnomial). Since p_1 is irreducible it is prime by the first bullet point on p.92 and thus $R/(p_1)$ is an integral domain. Hence $R/(p_1)[x]$ is also an integral domain. We must therefore have $\overline{a}(x) = 0$ or $\overline{b}(x) = 0$. That is, either p_1 divides every coefficient

of $a(x)$ or every coefficient of $b(x)$. Either way, we may divide $df(x) = a(x)b(x)$ through by p_1 to obtain

$$d'f(x) = a'(x)b'(x)$$

in which d' has one fewer irreducible factors than d. Repeating the argument, we arrive at an equation of the form $uf(x) = a''(x)b''(x)$ in $R[x]$ where u is a unit, and this case was already handled.

2. Again, we prove the contrapositive: if $f(x)$ is reducible in $R[x]$ then it is also reducible in $F[x]$. Suppose $f(x)$ factors nontrivially in $R[x]$ as $f(x) = g(x)h(x)$ with $g(x), h(x)$ non-units. If both g and h have positive degree, then they remain non-units in $F[x]$ and so $f(x)$ is reducible in that ring too. Otherwise, without loss, suppose $g(x)$ is the constant polynomial r. Then r must not be a unit in R and, since $f(x) = rh(x)$, the coefficients of $f(x)$ have a common factor of r, contrary to the assumption. □

In order to single out the class of polynomials that satisfy the assumptions of the second statement in the previous theorem it is useful to define the notion of content.

Definition 2.94. Suppose R is a UFD and $f(x) \in R[x]$. A *content of* $f(x)$, denoted $\text{cont}(f) \in R$, is a gcd of the coefficients of $f(x)$. We say $f(x)$ is *primitive* if $\text{cont}(f(x))$ is a unit. (Note that a content of f is a unit if and only if every other content of f is also a unit.)

Lemma 2.95. *Assume R is a UFD and $f(x), g(x) \in R[x]$. Then $f(x)$ and $g(x)$ are primitive if and only if $f(x)g(x)$ is primitive.*

Proof. Exercise. □

Theorem 2.96. *For a ring R, R is a UFD if and only if $R[x]$ is a UFD.*

Before proving it, notice that as an immediate Corollary we obtain:

Corollary 2.97. *If R is a UFD, then $R[x_1, \ldots, x_n]$ is a UFD for any n.*

So, for example, the Theorem justifies the fact that $F[x_1, \ldots, x_n]$, for a field F, and $\mathbb{Z}[x_1, \ldots, x_n]$ are UFD's.

January 11, 2018

Proof of Theorem 2.96. ($\Leftarrow$) We note that an element p of R is irreducible in R iff it is irreducible in $R[x]$ — this holds by degree considerations. Moreover, $R[x]^\times = R^\times$. It follows pretty quickly from these facts that if $R[x]$ is a UFD, then R is a UFD, but we skip the details.

($\Rightarrow$) The other implication is more interesting. Assume R is a UFD.

We first show factorizations exist. Let $f(x) \in R[x]$. Since R is UFD, we may consider its content $c = \text{cont}(f)$, so that $f(x) = cf'(x)$ with $f'(x)$ primitive. Now c factors in R into irreducibles and this remains an irreducible factorization of c in $R[x]$. So it suffices to prove $f'(x)$ has an irreducible factorization too.

Claim: Any primitive polynomial $f'(x)$ of positive degree in $R[x]$ factors as a product of primitive irreducible polynomials.

Proof of claim: If $f'(x)$ is irreducible, there is nothing to prove. Otherwise there is a non-trivial factorization $f'(x) = a(x)b(x)$, and since $f'(x)$ is primitive, we must have $\deg(a(x)) < \deg(f(x)), \deg(b(x)) < \deg(f(x))$. Moreover, by Lemma 2.95, each of $a(x)$ and $b(x)$ must also be primitive. The existence of irreducible factorizations for primitive polynomials thus follows by induction on degree.

For uniqueness, suppose we have two products of irreducible elements of $R[x]$ that are equal. Among the factors involved, we first write the constant factors and the the non-constant ones, getting an equation of the form

$$d_1 \cdots d_m p_1(x) \cdots p_n(x) = e_1 \cdots e_s q_1(x) \cdots q_t(x),$$

where d_i, e_j are irreducible elements of R and p_i, q_j are irreducible polynomials of degree at least one. Note that each of p_i, q_j must be primitive (since a non-primitive polynomial $p(x)$ factors as $\text{cont}(p)p'(x)$). By the Lemma, $p_1(x) \cdots p_n(x)$ and $q_1(x) \cdots q_t(x)$ are also primitive. It follows that $d_1 \cdots d_m$ is the content of $d_1 \cdots d_m p_1(x) \cdots p_n(x)$ and $e_1 \cdots e_m$ is the content $e_1 \cdots e_s q_1(x) \cdots q_t(x)$. Since these are equal, $d_1 \cdots d_m$ and $e_1 \cdots e_s$ agree up to a unit factor and hence, since R is a UFD, we have $s = m$ and, after reordering, d_i and e_i are associates, for all i.

We may now divide by $d_1 \ldots, d_m$ to get that

$$p_1(x) \cdots p_n(x) = u q_1(x) \cdots q_t(x)$$

for some unit u of R, and it remains to prove $n = t$ and, after reordering, that p_i and q_i are associates, for all i. Let F be the field of fractions of R. We know $F[x]$ is a Euclidean domain and hence it is a PID and hence a UFD. Moreover, by Gauss' Lemma, each p_i, q_j remains irreducible in $F[x]$. Thus $n = t$ and, after reordering, $p_i(x)$ and $q_i(x)$ are associate in $F[x]$, for all i. This means that for each i we have $p_i(x) = \frac{r_i}{s_i} q_i$, for some non-zero elements r_i, s_i of R, and hence $s_i p_i(x) = r_i q_i(x)$. But since p_i, q_j are primitive, we have $s_i = \text{cont}(s_i p_i(x))$ and $r_i = \text{cont}(r_i q_i(x))$. It follows that s_i and r_i are associates in R and hence $p_i = u q_i$ for some unit u. □

2.3.2 Irreducibility criteria for polynomials

We now discuss methods of determining irreducibility of polynomials. This is, in general, a difficult problem, but we will cover a few techniques that work in some cases.

We deal first with roots:

Definition 2.98. For a non-zero polynomial $f(x) \in F[x]$ and element $a \in F$, a is a root of f if $f(a) = 0$. The *multiplicity of a as a root of $f(x)$* is the greatest integer m such that $(x - a)^m$ divides $f(x)$.

Lemma 2.99. *Let F be a field and suppose $f(x) \in F[x]$. Then $f(x)$ has a degree one factor for the form $x - a$ for $a \in F$ if and only if $f(a) = 0$.*

Proof. Exercise on HW 1. □

Corollary 2.100. *A polynomial $f(x) \in F[x]$ of degree two or three is irreducible if and only if it has no roots.*

Proof. Assume f is non-constant of degree two or three. If f is irreducible, then it cannot have a root since otherwise we would have $f(x) = (x-a)g(x)$ with $\deg(g(x)) > 0$, by the Lemma 2.99. Conversely, if $f(x) = g(x)h(x)$ is a non-trivial factorization, then by degree considerations at least one of $g(x)$ or $h(x)$ has degree one, and thus is of the form $ax + b$ with $a \neq 0$. In this case $\frac{-b}{a}$ is a root of $f(x)$. □

Example. In $(\mathbb{Z}/5)[x]$, the polynomial $x^3 + x^2 + x + 3$ is irreducible. Just check all five possible elements of $\mathbb{Z}/5$ and observe that none of them is a root.

Remark 2.101. Never make the rookie mistake of thinking the previous corollary generalizes to higher degrees. For example, $(x^2 + 1)^2 \in \mathbb{R}[x]$ is a degree four polynomials without roots that is not irreducible.

January 14, 2019

Proposition 2.102 (Eisenstein's Criterion)**.** *Suppose R is an integral domain and let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in R[x]$ with $n \geq 1$. If there exists a prime ideal P of R such that $a_0, \ldots, a_{n-1} \in P$ and $a_0 \notin P^2$, then f is irreducible in $R[x]$.*

Proof. Suppose f were reducible. Since it is monic, we would be able to factor it as $f(x) = g(x)h(x)$, where $g(x)$ and $h(x)$ are polynomials in $R[x] \setminus R[x]^\times$. Since the leading coefficients of $\overline{g}$ and $\overline{h}$ multiply to 1, they are units in R. Thus we may assume that g and h are monic by multiplying each of these by the inverse of their leading coefficient.

Applying the reduction homomorphism $R[x] \to (R/P)[x]$ we have in the ring $(R/P)[x]$ the identity $x^n = \overline{f}(x) = \overline{g}(x)\overline{h}(x)$.

Set $T = R/P$ and notice that T is a domain. We now need an auxiliary claim.

Claim: If T is a domain and $\overline{g}(x), \overline{h}(x) \in T[x]$ are monic polynomials such that $\overline{g}(x)\overline{h}(x) = x^n$, then $\overline{g}(x) = x^m$ and $\overline{h}(x) = x^{n-m}$ for some $1 \leq m \leq n$.

Proof of claim: Let $g(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0$ and $h(x) = x^{n-m} + b_{n-m-1}x^{m-1} + \cdots + b_0$. Let j be the least integer such that $a_j \neq 0$ and i the least integer such that $b_i \neq 0$. (Set $a_m = 1 = b_{n-m}$.) The coefficient of x^{i+j} in $g(x)h(z)$ is $\sum_{s+t=i+j} a_s b_t$. The only non-zero term here is the term $a_j b_i$ (which is indeed non-zero since R is an integral domain), and hence the degree $i + j$ term of $g(x)h(x)$ is non-zero. This forces $i = m, j = n$.

The Claim thus gives that $\overline{g}$ and $\overline{h}$ have zero constant terms or, in other words, the constant terms of g and h are both in P. The constant term of $f = g \cdot h$ is thus in P^2, a contradiction. □

Corollary 2.103. *If R is UFD, such as $\mathbb{Z}$, then Eisenstein's Criterion gives: If $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in R[x]$ with $n \geq 1$ and there is a prime element p such that $p \mid a_i$ for $i = 0, \ldots n-1$, and $p^2 \nmid a_0$, then f is irreducible.*

Example. For example, $x^n - p \in \mathbb{Z}[x]$ is irreducible for all $n \geq 1$ and all primes p. By Gauss's Lemma, it is irreducible in $\mathbb{Q}[x]$ too. This implies, as an application of a homework problem that

$$\mathbb{Q}[x]/(x^n - p)$$

is a field. In fact, this field is isomorphic to $\mathbb{Q}(\sqrt[n]{p})$, the smallest subfield of $\mathbb{C}$ that contains $\mathbb{Q}$ and $\sqrt[n]{p}$.

Example. I claim the polynomial $f(x, y) = x^3 + y^5x + y$ is irreducible in $F[x, y]$ (where F is any field). To prove this, we make the identification $F[x, y] = R[x]$ where $R = F[y]$, so that $f = x^3 + r_1x + r_0$ where $r_1 = y^5$, $r_0 = y$. y is a prime element of R that divides r_1 and r_0, but y^2 does not divide r_0. So, by Eisenstein's Criterion, f is irreducible.

Chapter 3

Modules, Vector Spaces and Linear Algebra

3.1 Module theory

3.1.1 Definition and examples

Definition 3.1. Let R be a ring with $1 \neq 0$. A *left R-module* is an abelian group $(M, +)$ together with an action $R \times M \to M$ of R on M, written $(r, m) \mapsto rm$, such that for all $r, s \in R$ and $m, n \in M$

1. (r + s)m = rm + sm,
2. (rs)m = r(sm),
3. r(m + n) = rm + rn, and
4. 1m = m.

A *right R-module* is an abelian group $(M, +)$ with an action of R on M written as $M \times R \to M, (m, r) \mapsto mr$, such that for all $r, s \in R$ and $m, n \in M$

1. m(r + s) = mr + ms,
2. m(rs) = (mr)s,
3. (m + n)r = mr + nr, and
4. m1 = m.

Remark 3.2. For a ring R without 1, a left (right) R-module is an abelian group $(M, +)$ together with an action of R on M satisfying (1)-(3) of Def 3.1.

Convention: in this chapter, whenever we speak about R-modules we shall assume that the underlying ring R is unital.

Lemma 3.3 (Arithmetic in modules)**.** *Let R be a ring with $1_R \neq 0_R$ and let M be an R-module. Then $0_R m = 0_M$ and $(-1_R)m = -m$ for all $m \in M$.*

Remark 3.4. If R is a commutative ring, then any left R-module M may be regarded as a right R-module by setting $mr = rm$. Likewise, any right R-module may be regarded as a left R-module. Thus for commutative rings, we just refer to "modules", and not left or right modules.

January 16, 2019

To get some intuition on modules, we notice that all vector spaces (as encountered in an undergraduate algebra course) and all abelian groups are examples of modules.

Definition 3.5. Let F be a field. A *vector space* over F is an F-module.

Proposition 3.6. *Let M be a set with a binary operation $+$. Then*

1. *M is an abelian group if and only if M is a $\mathbb{Z}$-module.*
2. *M is an abelian group such that $nm := \underbrace{m + \cdots + m}_{n} = 0_M$ for all $m \in M$ if and only if M is a $\mathbb{Z}/n$-module.*

Proof. 1. If M is a module then $(M, +)$ is an abelian group by definition of module. Conversely, if $(M, +)$ is an abelian group then there is a unique $\mathbb{Z}$-module structure on M given by the formulas below. The uniqueness of the $\mathbb{Z}$ action follows from the identities below in which the right hand side is determined only by the abelian group structure of M. The various identities follow from the axioms of a module:

$$\begin{cases} i \cdot m = (\underbrace{1 + \cdots + 1}_{i}) \cdot m = \underbrace{1 \cdot m + \cdots + 1 \cdot m}_{i} = \underbrace{m + \cdots + m}_{i} & \text{if } i > 0 \\ 0 \cdot m = 0_M & \\ i \cdot m = -(-i) \cdot m = -(\underbrace{m + \cdots + m}_{-i}) & \text{if } i < 0. \end{cases}$$

It remains to check that this $\mathbb{Z}$-action really satisfies the module axioms. This is left as an exercise.

2. If M is a $\mathbb{Z}/n$ module then $(M, +)$ is an abelian group and $nm = \underbrace{m + \cdots + m}_{n} = \underbrace{[1]_n \cdot m + \cdots + [1]_n \cdot m}_{n} = [0]_n m = 0_M$. Conversely, there is a unique $\mathbb{Z}/n$-module structure on M given by the formulas analogous to the ones above

$$\begin{cases} [i]_n \cdot m = (\underbrace{[1]_n + \cdots + [1]_n}_{i}) \cdot m = \underbrace{[1]_n \cdot m + \cdots + [1]_n \cdot m}_{i} = \underbrace{m + \cdots + m}_{i} & \text{if } i > 0 \\ 0 \cdot m = 0_M & \\ [i]_n \cdot m = -(-[i]_n) \cdot m = -(\underbrace{m + \cdots + m}_{-i}) & \text{if } i < 0. \end{cases}$$

These formulas are well defined, that is, independent of the choice of coset representative for $[i]_n$, because of the assumption $nm = 0_M$. Again checking that this $\mathbb{Z}/n$-action really satisfies the module axioms is left as an exercise. □

The proposition above says in particular that any group of the form $G = \mathbb{Z}^\ell \times \mathbb{Z}/d_1 \times \cdots \times \mathbb{Z}/d_m$ is a $\mathbb{Z}$-module and if $\ell = 0, m \geq 1$ and $d_i \mid n$ for $1 \leq i \leq m$ then G is also a $\mathbb{Z}/n$-module. In particular, the Klein group is a $\mathbb{Z}/2$-module.

Note that in contrast to vector spaces for a module M over a ring R it can happen that $rm = 0$ for some $r \in R$, $m \in M$ such that $r \neq 0_R$ and $m \neq 0_M$. For example in the Klein group K_4 viewed as a $\mathbb{Z}$-module we have $2m = 0$ for all $m \in K_4$.

Further examples of modules include:

Example.

- The trivial module is $0 = \{0\}$ with $r0 = 0$ for any $r \in R$.
- If R is a ring then R is a left and right an R-module via the action of R on itself given by its internal multiplication.
- If I is a left (right) ideal of a ring R then I is a left (right) R-module with respect to the action of R on I by internal multiplication.
- If S is a subring of a ring R then R is an S-module with respect to the action of S on R by internal multiplication in R.
- If R is a commutative ring with $1 \neq 0$ then $R[x_1, \ldots, x_n]$ is an R-module for any $n \geq 1$.
- If R is a commutative ring then $M_n(R)$ is is an R-module for $n \geq 1$.
- If R is a commutative ring and G is a group then $R[G]$ is an R-module.
- The free R-module of rank n is the set

$$R^n = \left\{ \begin{bmatrix} r_1 \\ \vdots \\ r_n \end{bmatrix} \mid r_i \in R, 1 \leq i \leq n \right\}$$

  with componentwise addition and multiplication by elements of R

$$\begin{bmatrix} r_1 \\ \vdots \\ r_n \end{bmatrix} + \begin{bmatrix} r_1' \\ \vdots \\ r_n' \end{bmatrix} = \begin{bmatrix} r_1 + r_1' \\ \vdots \\ r_n + r_n' \end{bmatrix} \text{ and } r \begin{bmatrix} r_1 \\ \vdots \\ r_n \end{bmatrix} = \begin{bmatrix} rr_1 \\ \vdots \\ rr_n \end{bmatrix}.$$

For an R-module M the ring R is often referred to as the ring of scalars (by analogy to the vector space case). Given an action of a ring of scalars on a module, we can sometimes produce an action of a different ring of scalars on the same set, producing in effect a new module structure.

Proposition 3.7 (Restriction of scalars)**.** *Let $\phi : R \to S$ be a ring homomorphism of unital rings such that $\phi(1_R) = 1_S$. Any left S-module M may be regarded via "restriction of scalars" as a left R-module with R-action defined by $rm := \phi(r)m$ for*

any $m \in M$. In particular, if R is a subring of a ring S then any left R-module M may be regarded via "restriction of scalars" as a left S-module with S-action defined by the action of the elements of s viewed as elements of R.

Proof. Let $r, s \in R$ and $m, n \in M$. One checks that the properties in the definition of module hold for the given action using properties of ring homomorphisms. For example:

$$(r+s)m = \phi(r+s)m = (\phi(r) + \phi(s))m = \phi(r)m + \phi(s)m = rm + sm.$$

□

Example.
- If I is an ideal of a ring R then applying restriction of scalars along the quotient homomorphism $q : R \to R/I$ gives that any left R/I-module is also a left R-module.
- In particular, applying this to the R/I-module R/I gives that makes R/I is a left and right R-module by restriction of scalars along the quotient homomorphism.

Definition 3.8. Let R be a ring and let M be a left R-module. An *R-submodule* of M is a subgroup $N \leq M$ satisfying $rn \in N$ for all $r \in R$ and $n \in N$.

Lemma 3.9 (One-step test for submodules)**.** *Let R be a ring with $1 \neq 0$ and let M be a left R-module. A nonempty subset N of M is an R-submodule of M if and only if $rn + n' \in N$ for all $r \in R$ and $n, n' \in N$.*

Example.
- Let R be a ring and let M be a subset of R. Then M is a left (right) R-submodule of R if and only if M is a left (right) ideal of R.
- Let R be a commutative ring with $1 \neq 0$, let I be an ideal of R and let M be an R-module. Then $IM := \{\sum_{k=1}^{n} j_k m_k \mid n \geq 0, j_k \in I, m_k \in M \text{ for } 1 \leq k \leq n\}$ is a submodule of M.

January 18, 2019

3.1.2 Module homomorphisms and isomorphisms

Definition 3.10. Let R be a ring and let M and N be R-modules. An *R-module homomorphism* from M to N is a function $h : M \to N$ such that for all $r \in R$ and $m, n \in M$

1. $h(m+n) = h(m) + h(n)$, i.e. h is an additive group homomorphism, and
2. $h(rm) = rh(m)$.

Definition 3.11. An R-module homomorphism h is an *R-module isomorphism* if h is also a bijection.

Definition 3.12. Let F be a field and let M and N be vector spaces over F. A *linear transformation* from M to N is an F-module homomorphism $h : M \to N$.

Lemma 3.13. *Let R be a ring with $1 \neq 0$ and let M be an R-module.*

1. *Let N be an R-submodule of M. Then the inclusion map $i : N \to M$ is an R-module homomorphism.*
2. *If $h : M \to M'$ is an R-module homomorphism, then $\mathrm{Ker}(h)$ is an R-submodule of M and $\mathrm{Im}(h)$ is an R-submodule of M'.*

Proof. Exercise. □

Definition 3.14. Let R be a ring and let M and N be R-modules. Then $\mathrm{Hom}_R(M, N)$ denotes the set of all R-module homomorphisms from M to N, and $\mathrm{End}_R(M)$ denotes the set $\mathrm{Hom}_R(M, M)$. $\mathrm{End}(M)$ is called the *endomorphism ring* of M, and elements of $\mathrm{End}(M)$ are called *endomorphisms*.

Example. We will see later that for an n-dimensional vector space V over a field F, $\mathrm{End}_F(V) \cong M_n(F)$, that is every linear transformation $T : V \to V$ corresponds to an $n \times n$ matrix.

Example. For any commutative ring R with $1 \neq 0$ and any R-module M there is an isomorphism of R-modules $\mathrm{Hom}_R(R, M) \cong M$.

Proof. Let $f : M \to \mathrm{Hom}_R(R, M)$ be given for each $m \in M$ by $r(m) = \phi_m$ where $\phi_m(r) = rm$ for all $r \in R$. Then

- f is well defined, i.e. for any $m \in M$ ϕ_m is an element of $\mathrm{Hom}_R(R, M)$ since

$$\phi_m(r_1 + r_2) = (r_1 + r_2)m = r_1m + r_2m = \phi_m(r_1) + \phi_m(r_2)$$

$$\phi_m(r_1r_2) = (r_1r_2)m = r_1(r_2m) = r_1\phi_m(r_2)$$

  for all $r_1, r_2 \in R$.

- f is an R-module homomorphism since one can verify that

$$\phi_{m_1+m_2}(r) = r(m_1 + m_2) = rm_1 + rm_2 = \phi_{m_1}(r) + \phi_{m_2}(r)$$

$$\phi_{r'm}(r) = r(r'm) = (rr')m = r'(rm) = r'\phi_m(r)$$

- f is injective since $\phi_m = \phi'_m$ implies $\phi_m(1_R) = \phi'_m(1_R)$, i.e. $m = m'$.
- f is surjective since for $\psi \in \mathrm{Hom}_R(R, M)$ we have $\psi(r) = \psi(r1_R) = r\psi(1_R)$ for all $r \in R$, so $\psi = \phi_{\psi(1_R)}$.

This shows that f is an R-module isomorphism. □

Definition 3.15. Let R be a commutative ring with $1_R \neq 0_R$. An *R-algebra* is a ring A with $1_A \neq 0_A$ together with a ring homomorphism $f : R \to A$ such that $f(1_R) = 1_A$ and $f(R)$ is contained in the center of A.

Example. Let R be a commutative ring with $1_R \neq 0_R$. The following are R-algebras: $R[x_1, \ldots, x_n$ (with the inclusion $R \hookrightarrow R[x_1, \ldots, x_n)$, $M_n(R)$ (with the homomorphism $r \mapsto rI_n$), R[G] for any group G (with the inclusion $R \hookrightarrow R[G], r \mapsto re_G$).

Proposition 3.16. *Let R be a commutative ring with $1 \neq 0$ and let M and N be R-modules. Then*

1. $\mathrm{Hom}_R(M, N)$ *is an R-module with addition and R-action defined by*

$$(f + g)(m) = f(m) + g(m) \text{ and } (rf)(m) = r(f(m))$$

   for all $f, g \in \mathrm{Hom}_R(M, N), m \in M, r \in R$.

2. $\mathrm{End}_R(M)$ *is an R-algebra, with addition and R-action defined as above, and multiplication defined by composition $(fg)(m) = f(g(m))$ for all $f, g \in \mathrm{End}_R(M)$ and all $m \in M$.*

Proof. There are many things to check here, including that:

- the addition and R-action are well defined i.e. if $f, g \in \mathrm{Hom}_R(M, N)$ and $r \in R$ then $f + g, rf \in \mathrm{Hom}_R(M, N)$
- the axioms of an R-module are satisfied for $\mathrm{Hom}_R(M, N)$
- additionally, the axioms of a unital ring are satisfied for $\mathrm{End}_R(M)$
- there is a ring homomorphism $f : R \to \mathrm{End}_R(M)$ such that $f(1_R) = 1_{\mathrm{End}_R(M)} = \mathrm{id}_M$ and $f(R) \subseteq Z(\mathrm{End}_R(M))$.

We'll just check the last item and let the others be exercises. Define $f : R \to \mathrm{End}_R(M)$ by $f(r) = r\mathrm{id}_M$. Then $f(r + s) = (r + s)\mathrm{id}_M = r\mathrm{id}_M + s\mathrm{id}_M = f(r) + f(s)$ and $f(rs) = (rs)\mathrm{id}_M = (r\mathrm{id}_M) \circ (s\mathrm{id}_M) = f(r)f(s)$ show that f is a ring homomorphism and further it is clear since $\mathrm{id}_M \in Z(\mathrm{End}_R(M))$ that $f(R) \subseteq \mathrm{End}_R(M)$. □

January 23, 2019

Remark 3.17. Let R be a commutative ring with $1 \neq 0$ and let M be an R-module. Then M is also an $(\mathrm{End}_R(M))$ module with the action $\phi m = \phi(m)$ for any $\phi \in \mathrm{End}_R(M)$, $m \in M$.

We come to a very important class of examples which will help us study linear transformations using module theory.

Proposition 3.18 ($F[x]$-modules)**.** *Let F be a field. There is a bijection*

$$\{V \text{ an } F[x]\text{-module}\} \longleftrightarrow \{V \text{ an } F\text{-vector space and } T \in \mathrm{End}_F(V)\}.$$

Proof. If V is an $F[x]$ module then V is an F-vector space by restriction of scalars along the inclusion $F \hookrightarrow F[x]$. Let $T : V \to V$ be defined by $T(v) = xv$. It can be shown that $T \in \mathrm{End}_F(V)$ since $T(v_1+v_2) = x(v_1+v_2) = xv_1+xv_2 = T(v_1)+T(v_2)$ and $T(cv) = x(cv) = c(xv)$ for any $c \in F$, $v, v_1, v_2 \in V$ by the axioms of the $F[x]$-module.

Conversely, let V be an F-vector space and $T \in \mathrm{End}_F(V)$. Consider the evaluation homomorphism $\varphi : F[x] \to \mathrm{End}_F(V), \quad \varphi(f(x)) = f(T)$. (For example, if $f(x) = x^2+5$ then $\varphi(f(x)) = T \circ T + 5 \cdot \mathrm{id}_V$.) Since V is an $\mathrm{End}_F(V)$-module by Remark 3.17, then V is also an $F[x]$-module by restriction of scalars along ϕ. Concretely, this action is given by

$$f(x)v = (f(T))(v).$$

(For example, if $f(x) = x^2 + 5$, then $f(x)v = T(T(v)) + 5v$.) □

Notation 3.19. We shall denote the $F[x]$-module structure on an F-vector space V induced by $T \in \mathrm{End}_F(V)$ by V_T.

Example. The proposition above says that if we fix an F-vector space V then any linear transformation T gives a different $F[x]$ module structure on V. For example,

- for $T = 0$ the $F[x]$ module V_0 carries an action given by scaling by the constant coefficient of f, that is if $f(x) = a^n x^n + \cdots + a_0$ then

$$f(x)v = (f(0))v = a_0 v \text{ for all } f \in F[x].$$

- for T the "shift opearator" that takes $T(e_i) = e_{i-1}$, where e_i is the i-th standard basis vector, the $F[x]$ module V_T is has the action $x^m \begin{bmatrix} v_1 \\ \vdots \\ v_{n-m} \\ v_{n-m+1} \\ \vdots \\ v_n \end{bmatrix} = \begin{bmatrix} v_{m+1} \\ \vdots \\ v_n \\ 0 \\ \vdots \\ 0 \end{bmatrix}$.

Definition 3.20. Let R be a ring, let M be an R-module, and let N be a submodule of M. The quotient module M/N is the quotient group M/N with R action defined by

$$r(m + N) = rm + N$$

for all $r \in R$ and $m + N \in M/N$.

Lemma 3.21. *Let R be a ring, let M be an R-module, and let N be a submodule of M. The quotient module M/N is an R-module, and the quotient map $q : M \to M/N$ is an R-module homomorphism with kernel* $\mathrm{Ker}(q) = N$.

Proof. Among the many things to check here we will only check the well-definedness of the R-action on M. If $m+N = m'+N$ then $m-m' \in N$ so $r(m-m') \in N$ by the definition of submodule. This gives that $rm - rm' \in N$, hence $rm+N = rm'+N$. $\square$

Example. If R is a field, submodules and quotient modules are the same things as sub and quotient vector spaces.

If $R = \mathbb{Z}$, then recall that $\mathbb{Z}$-modules are the same as abelian groups. Submodules and quotient $\mathbb{Z}$-modules are the same things as subgroups and quotients of abelian groups.

Theorem 3.22 (Module Isomorphism Theorems)**.** *: Let R be a ring, and let M be an R-module.*

1. *(First Isomorphism Theorem) Let N be an R-module and let $h : M \to N$ be an R-module homomorphism. Then* $\mathrm{Ker}(h)$ *is a submodule of M and there is an R-module isomorphism $M/\mathrm{Ker}(h) \cong h(M)$.*

2. *(Second Isomorphism Theorem) Let A and B be submodules of M, and let $A+B = \{a+b \mid a \in A, b \in B\}$. Then $A+B$ is a submodule of M, $A \cap B$ is a submodule of A, and there is an R-module isomorphism $(A+B)/B \cong A/(A \cap B)$.*

3. *(Third Isomorphism Theorem) Let A and B be submodules of M with $A \subseteq B$. Then there is an R-module isomorphism $(M/A)/(B/A) \cong M/B$.*

4. *(Lattice Isomorphism Theorem) Let R be a ring, let N be a R-submodule of an R-module M, and let $q : M \to M/N$ be the quotient map. Then the function*

$$\Psi : \{R - \textit{submodules of } M \textit{ containing } N\} \to \{R - \textit{submodules of } M/N\}$$

defined by $\Psi(K) = q(K) = K/N$ is a bijection with inverse defined by $\Psi^{-1}(T) = q^{-1}(T)$ for each R-submodule T of M/N. Moreover, Ψ and Ψ^{-1} preserve sums and intersections.

January 25, 2019

3.1.3 Module generators, bases and free modules

Definition 3.23. Let M be an R-module. A *linear combination* of finitely many elements $a_1, ..., a_n$ of M is an element of M of the form $r_1 m + 1 + \cdots + r_n m_n$ for some $r_1, \ldots, r_n \in R$.

Let's talk about the set of all linear combinations that can be obtained starting from a given set.

Definition 3.24. Let R be a ring with $1 \neq 0$ and let M be an R-module. For a subset A of M, the submodule of M *generated by* A is $RA = \{r_1a_1 + \cdots + r_na_n \mid n \geq 0, r_i \in R, a_i \in A\}$. M is said to be generated by A if $M = RA$.

A module M is *finitely generated* if there is a finite subset A of M that generates M. If $A = a$ has a single element, the module $RA = Ra$ is called *cyclic*.

Remark 3.25. If M is an F-vector space we say say that M is *spanned by* a set A instead of generated by A.

Lemma 3.26. *Let M be an R-module and let $A \subseteq M$. Then RA is the smallest submodule of M containing A, that is*

$$RA = \bigcap_{A \subseteq N, N \text{ submodule of } M} N.$$

Lemma 3.27. *Being finitely generated and being cyclic are R-module isomorphism invariants.*

Example. Let R be a ring with $1 \neq 0$.

- $R = R1$ is cyclic.
- $R \oplus R$ is generated by $\{(1, 0), (0, 1)\}$.
- $R[x]$ is generated as an R-module by the set $MM(x) = \{1, x, x^2, \ldots, x^n, \ldots\}$ of monic monomials in the variable x.
- Let $M = \mathbb{Z}[x, y]$. M is generated by
  - $\{1, x, y\}$ as a ring,
  - $MM(y) = \{1, y, y^2, \ldots, y^n, \ldots\}$ as an $\mathbb{Z}[x]$-module, and
  - $MM(x, y) = \{x^i y^j \mid i, j \in \mathbb{Z}_{\geq 0}\}$ as a group ($\mathbb{Z}$-module).

Lemma 3.28. *Let R be a ring with $1 \neq 0$, let M be an R-module, and let N be an R-submodule of M.*

1. *If M is finitely generated as an R-module, then so is M/N.*
2. *If N and M/N are finitely generated as R-modules, then so is M.*

Proof. 1. If $M = RA$ then $M/N = R\bar{A}$, where $\bar{A} = \{a + N \mid a \in A\}$.

2. Homework exercise. □

Definition 3.29. Let M be an R-module and let A be a subset of M. The set A is *linearly independent* if whenever $r_1, \ldots, r_n \in R$ and $a_1, \ldots, a_n$ are distinct elements of A satisfying $r_1a_1 + \cdots + r_na_n = 0$, then $r_1 = \cdots = r_n = 0$. Otherwise A is *linearly dependent*.

Definition 3.30. A subset A of an R-module M is a *basis* of M, if the set A generates M and is linearly independent. An R-module M is a *free* R-module if M has a basis.

Example. All of the following modules are free.

- $\{1\}$ is a basis for R
- $\{(1,0),(0,1)\}$ is a basis for $R \oplus R$
- $MM(x) = \{1, x, x^2, \ldots, x^n, \ldots\}$ is a basis for $R[x]$.
- Let $M = \mathbb{Z}[x,y]$. $MM(y) = \{1, y, y^2, \ldots, y^n, \ldots\}$ is a basis for the $\mathbb{Z}[x]$-module M and $MM(x,y) = \{x^i y^j \mid i,j \in \mathbb{Z}_{\geq 0}\}$ is a basis for the $\mathbb{Z}$-module M.

Example. $\mathbb{Z}/2$ is not a free $\mathbb{Z}$-module. Indeed suppose that A is a basis for $\mathbb{Z}/2$ and $a \in A$. Then $2a = 0$ so A cannot be linearly independent, a contradiction.

Lemma 3.31. *If A is a basis of M then every nonzero element $0 \neq m \in M$ can be written uniquely as $m = r_1 a_1 + \cdots + r_n a_n$ with a_i distinct elements of A and $r_i \neq 0$.*

Theorem 3.32 (UMP for free R-modules)**.** *Let R be a ring, let M be a free R-module with basis B, let N be an R-module, and let $j : B \to N$ be any function. Then there is a unique R-module homomorphism $h : M \to N$ such that $h(b) = j(b)$ for all $b \in B$.*

January 28, 2019

Proof of 3.31. Suppose that if $m \neq 0$ and A_1, A_2 are finite subsets of A such that

$$m = \sum_{a \in A_1} r_a a = \sum_{b \in A_2} s_b b.$$

Then

$$\sum_{a \in A_1 \cap A_2} (r_a - s_a)a + \sum_{b \in A_1 \setminus A_2} r_b b - \sum_{c \in A_2 \setminus A_1} r_c c = 0$$

which yileds by linear independence of A that $r_a = s_a$ for $a \in A_1 \cap A_2$, $r_b = s_c = 0_R$ for $b \in A_1 \setminus A_2$ and $c \in A_2 \setminus A_1$. Set $A' = \{a \in A_1 \cap A_2 \mid r_s \neq 0_R\}$. Then $m = \sum_{a \in A'} r_a a$ is the unique way of writing m as given in the statement of the lemma. □

Proof of Theorem 3.32. Existence: By Lemma 3.31 any $0 \neq m \in M$ can be written uniquely as $m = r_1 b_1 + \cdots + r_n b_n$ with $b_i \in B$ distinct and $0 \neq r_i \in R$. Define $h : M \to N$ by

$$\begin{cases} h(r_1 b_1 + \cdots + r_n b_n) = r_1 j(b_1) + \cdots + r_n j(b_n) & \text{if } r_1 b_1 + \cdots + r_n b_n \neq 0 \\ h(0_M) = 0_N \end{cases}$$

One can check that this satisfies the conditions to be an R-module homomorphism. *Uniqueness:* Let $h : M \to N$ be an R-module homomorphism such that $h(b_i) = j(b_i)$.

Then in particular $h : (M, +) \to (N, +)$ is a group homomorphism and therefore $h(0_m) = 0_N$ by properties of group homomorphisms. Furthermore, if $m = r_1b_1 + \cdots + r_nb_n$ then $h(m) = h(r_1b_1 + \cdots + r_nb_n) = r_1h(b_1) + \cdots + r_nh(b_n) = r_1j(b_1) + \cdots + r_nj(b_n)$ by the definition of homomorphism and because $h(b_i) = j(b_i)$. □

Corollary 3.33. *If A and B are sets of the same cardinality, i.e. related by a set theoretic isomorphism $j : A \to B$ and M and N are free R-modules with bases A and B respectively, then $M \cong N$ as R-modules.*

Proof. Let $h : M \to N$ and $h' : N \to M$ be the module homomorphisms induced by the bijection $j : A \to B$ and its inverse $j^{-1} : B \to A$ by the UMP for free modules. We'll show that h and h' are mutual inverses. For this note that $h \circ h' : N \to N$ is an R-module homomorphism and $(h \circ h')(b) = h(j(b)) = j^{-1}(j(b)) = b$ for every $b \in B$. Since the identity map id_N is an R-module homomorphism and $id_N(n) = b$ for every $b \in B$, by the uniqueness in the UMP we have $h \circ h' = \mathrm{id}_n$. Similarly $h' \circ h = \mathrm{id}_M$. □

The corollary gives that there is only one (up to isomorphism) free module with basis A, provided such a module exists. But does a free module generated by a given set A exist? It turns out it does.

Definition 3.34. Let R be a ring and let A be a set. The free R-module generated by A, denoted $F_R(A)$ is the set of formal sums

$$\begin{aligned} F_R(A) &= \{r_1a_1 + \cdots + r_na_n \mid n \geq 0, r_i \in R, a_i \in A\} \\ &= \{\sum_{a \in A} r_a a \mid r_a \in R, r_a = 0 \text{ for all but finitely many } a\}, \end{aligned}$$

with addition defined by

$$(\sum_{a \in A} r_a a) + (\sum_{a \in A} s_a a) = \sum_{a?A} (r_a + s_a)a$$

and R-action defined by

$$r(\sum_{a \in A} r_a a) = \sum_{a \in A} (rr_a)a.$$

Remark 3.35.

- $F_R(A)$ is an R-module
- $F_R(A)$ is a free module with basis A (to be shown on homework).
- $F_R(A) \cong \bigoplus_{a \in A} R$ (to be shown on homework).

Theorem 3.36 (Uniqueness of rank over commutative rings)**.** *Let R be a commutative ring with $1 \neq 0$ and let M be a free R-module with bases A and B. Then A and B have the same cardinality, i.e. they are related by a bijection.*

Proof. Homework. □

Definition 3.37. Let R be a commutative ring with $1 \neq 0$ and let M be a free R-module. The cardinality of any basis of M is called the *rank* of M.

Example. Let R be a commutative ring with $1 \neq 0$. The rank of R^n is n.

January 30, 2018

Definition 3.38. Let R be a ring. Let M_α be R-modules for all α in an index set J. The *direct product* of the R-modules M_α is the Cartesian product $\prod_{\alpha\in J} M_a$ with addition defined by

$$(m_\alpha)_{\alpha\in J} + (n_\alpha)_{\alpha\in J} = (m_\alpha + n_\alpha)_{\alpha\in J}$$

and R-action defined by

$$r(m_\alpha)_{\alpha\in J} = (rm_\alpha)_{\alpha\in J}.$$

The *direct sum* of the R-modules M_α is the R-submodule $\bigoplus_{\alpha\in J} M_\alpha$ of the direct product $\prod_{\alpha\in J} M_a$ given by

$$\bigoplus_{\alpha\in J} M_\alpha = \{(m_\alpha)_{\alpha\in J} \mid m_\alpha = 0 \text{ for all but finitely many } \alpha\}.$$

Lemma 3.39. *The direct sum and the direct product of an arbitrary family of R-modules are in their turn R-modules.*

Example. Suppose that $|A| = n < \infty$. Let $M_1, \ldots, M_n$ be R-modules. The *direct product module* $M_1 \times \cdots \times M_n$ is the abelian group $M_1 \times \cdots \times M_n$ with ring action given by $r(m_1, \ldots, m_n) = (rm_1, \ldots, rm_n))$ for all $r \in R$ and $m_i \in M_i$. Comparing the definitions we see that

$$M_1 \times \cdots \times M_n = M_1 \oplus \cdots \oplus M_n.$$

If $M_i = R$ for $1 \leq i \leq n$, then we denote $R^n = \underbrace{R \times \cdots \times R}_{n} = \underbrace{R \oplus \cdots \oplus R}_{n}$.

It is useful to talk about maps from the factors/summands to the direct product/ direct sum and conversely.

Definition 3.40. For $i \in J$ the *inclusion of the i-th factor* into a direct product or direct sum is the map

$$\iota_i : M_i \to \prod_{\alpha\in J} M_\alpha \text{ or } \iota_i : M_i \to \bigoplus_{\alpha\in J} M_a, \iota_i(m) = (m_\alpha)_{\alpha\in J}, \text{ where } m_\alpha = \begin{cases} m & \text{if } \alpha = i \\ 0 & \text{if } \alpha \neq i \end{cases}.$$

For $i \in J$ the i-th *projection map* from a direct product or a direct sum module is

$$\pi_i : \prod_{\alpha\in J} M_a \to M_i \text{ or } \pi_i : \bigoplus_{\alpha\in J} M_a \to M_i, \pi_i\left((m_\alpha)_{\alpha\in J}\right) = m_i.$$

Lemma 3.41. *Projections from direct products or sums of R-module, inclusions into direct products or sums of R-modules, and products of R-module homomorphisms are R-module homomorphisms. Furthermore inclusions are injective, projections are surjective and $\pi_i \circ \iota_i = id_{M_i}$ (but $\iota_i \circ \pi_i \neq id$). Also $\iota_i(M_i)$ is an R-submodule of the direct product/sum which is isomorphic to M_i.*

3.2 Vector spaces and linear transformations

3.2.1 Classification of vector spaces and dimension

In this section we will first show that every vector space has a basis and all bases of a given vector space have the same cardinality.

Recall that for a subset A of an F-vector space V, the *span* of A, denoted $\mathrm{Span}(A)$ is the subspace generated by A, i.e. $\mathrm{Span}(A) = \{\sum_{i=1}^{n} c_i a_i \mid n \geq 0, c_i \in F, a_i \in A\}$.

Lemma 3.42. *Suppose I is a linearly independent subset of an F-vector space V and $v \in V \setminus \mathrm{Span}(I)$, then $I \cup \{v\}$ is also linearly independent.*

Proof. Let $w_1, \ldots, w_n$ be any list of distinct elements of $I \cup \{v\}$ and suppose with $\sum_i c_i w_i = 0$ for some $c_i \in F$. If none of the w_i's is equal to v then $c_i = 0$ for all i since I is linearly independent. Without loss, say $w_1 = v$. If $c_1 = 0$ then $c_i = 0$ for all i by the same reasoning as in the previous case. If $c_1 \neq 0$, then $v = \sum_{i \geq 2} c_i/c_1 w_i \in \mathrm{Span}(I)$, contrary to assumption. This proves $I \cup \{v\}$ is a linearly independent set. □

Theorem 3.43 (Every vector space has a basis)**.** *Let V be an F-vector space and assume $I \subseteq S \subseteq V$ are subsets such that I is linearly independent and S spans V. Then there is a subset B with $I \subseteq B \subseteq S$ such that B is a basis.*

The rigorous proof of the Theroem needs Zorn's Lemma 2.56. But let's first give a heuristic proof: Start with I. If $\mathrm{Span}(I) = V$, then $B = I$ does the job. If not, then since $\mathrm{Span}(S) = V$, there must be a $v \in S \setminus \mathrm{Span}(I)$. Let $I' := I \cup \{v\}$. Then $I' \subseteq S$ and, by Lemma 3.42, I' is linearly independent. If $\mathrm{Span}(I') = V$, we have found our B, and if not we construct I'' from I' just as we constructed I' from I. At this point we'd like to say that this process cannot go on for ever, and this is more-or-less true. But at least in an infinite dimensional setting, we need to use Zorn's Lemma.

Before proving the theorem, let's look at an important consequence:

Corollary 3.44. *Every F vector space V has a basis. Moreover, every linearly indendent subset of V is contained in some basis, and every set of vectors that spans V contains some basis.*

Proof of Corollary. For this first part, apply the theorem with $I = \emptyset$ and $S = V$. For the second and third, use I arbitrary and $S = V$ and $I = \emptyset$ and S arbitrary, respectively. □

Example. $\mathbb{R}$ has a basis as a $\mathbb{Q}$-vector space. Just don't ask me what it looks like.

February 1, 2019

Remark 3.45. Some mathematicians refuse to accept Zorn's Lemma into their axiom system. We will at least pretend to be mathematicians who do.

Proof of Theorem 3.43. Let $\mathcal{P}$ denote the collection of all subsets X of V such that $I \subseteq X \subseteq S$ and X is linearly independent. We make $\mathcal{P}$ into a poset by the order relation $\subseteq$, set containment.

We note that $\mathcal{P}$ is not empty since, for example $I \in \mathcal{P}$.

Let $\mathcal{T}$ be any non-empty chain in $\mathcal{P}$. Let $Z = \bigcup_{Y \in \mathcal{T}} Y$. I claim $Z \in \mathcal{P}$. Given $z_1, \ldots, z_m \in Z$, for each i we have $z_i \in Y_i$ for some $Y_i \in T$. Since T is totally ordered, one of $Y_1, \ldots, Y_m$ contains all the others and hence contains all the z_i's. Since Y_i is linearly independent, this shows $z_1, \ldots, z_m$ are lineraly independent. Thus Z is linearly indendent. Since $\mathcal{T}$ is non-empty, $Z \supseteq I$ and hence $Z \in \mathcal{P}$. It is clearly an upper bound for $\mathcal{T}$.

By Zorn's Lemma, $\mathcal{P}$ has a maximal element B, and I claim it is a basis of V. Note that B is linearly independent and $I \subseteq B \subseteq S$ by construction. We need to show that it spans. Suppose not. Since S spans V, if $S \subseteq \mathrm{Span}(B)$, then $\mathrm{Span}(B)$ would have to be all of V. So, there is at least one $v \in S$ such that $v \notin \mathrm{Span}(B)$, and set $X := B \cup \{v\}$. Clearly, $I \subset X \subseteq S$ and, by Lemma 3.42, X is linearly independent. This shows that X is an element of $\mathcal{P}$ that is strictly bigger than B, contrary to the maximality of B. □

Definition 3.46. An F vector space is *finite dimensional* if there is a finite subset that spans it. Thanks to the Theorem 3.43, this is equivalent to the property that it has a finite basis.

The following is an essential property of vector spaces that eventually will allow us to compare bases in terms of size.

Lemma 3.47 (Exchange Property)**.** *Let B be a basis of a vector space V and let $C = \{c_1, \ldots, c_m\}$ be any (finite) set of linearly independent vectors in V. Then there are distinct vectors $b_1, \ldots, b_m$ in B such that $(B \setminus \{b_1, \ldots, b_m\}) \cup C$ is also a basis V.*

Proof. I will prove by induction on k, where $0 \leq k \leq m$, that for each k with $0 \leq k \leq m$ there are distinct vectors $b_1, \ldots, b_k$ in B such that $(B \setminus \{b_1, \ldots, b_k\}) \cup \{c_1, \ldots, c_k\})$ is also a basis of V. The base case, $k = 0$, is clear. The terminal case, $k = m$, gives us the desired statement.

For the inductive step, assume $B' = (B \setminus \{b_1, \ldots, b_k\}) \cup \{c_1, \ldots, c_k\})$ is also a basis of V. Since $c_{k+1} \in V$ we can write

$$c_{k+1} = \sum_{i=1}^{n} \lambda_i b_i + \sum_{i=1}^{k} \mu_i c_i$$

for some scalars $\lambda_i, \mu_i \in F$ and some elements $b_i \in B \setminus \{b_1, \ldots, b_k\}$. Note that since C is linearly independent at least one of the scalars λ_i is nonzero. Let i_0 be such that $\lambda_{i_0} \neq 0$ and notice that solving for b_{i_0} from the displayed equation gives that $b_{i_0} \in \mathrm{Span}(B'')$ where $B'' = (B' \setminus \{b_{i_0}\}) \cup \{c_{k+1}\})$. Now we can "replace" b_{i_0} by c_k since the previous statement implies $\mathrm{Span}(B'') = \mathrm{Span}(B') = V$ and moreover B'' is linearly independent since otherwise B' would be linearly dependent (details left to the reader). □

Theorem 3.48 (Dimension Theorem)**.** *Any two bases of the same (possibly infinite dimensional) vector space have the same cardinality.*

Proof. We will only prove this under the assumption that V is finite dimensional.

Suppose V is finite dimensional. Then it has a finite basis B. Let B' be any other basis. (Note that we cannot assume B' is necessarily finite.) Let $\{c_1, \ldots, c_m\}$ be any m-element subset of B' for any m. An immediate consequence of Lemma 3.47 is that $m \leq |B|$ (since otherwise we could not find m distinct elements of B to replace the c_i's by). Since every finite subset of B' has cardinality no larger than $|B|$ this proves that B' is finite and $|B'| \leq |B|$. By symmetry, we obtain $|B| \leq |B|'$ too, hence equality follows. □

Definition 3.49. The *dimension* of a vector space V, denoted $\dim_F(V)$ or $\dim(V)$, is the cardinality of any of its bases.

Example. $\dim_F(F^n) = |\{e_1, e_2, \ldots, e_n\}| = n$.

Theorem 3.50 (Classification of finitely generated vector spaces)**.** *Let F be a field.*

1. *Every finitely generated vector space over F is isomorphic to F^n for $n = \dim_F(V)$.*
2. *For any $m, n \in \mathbb{Z}_{\geq 0}$, $F^m \cong F^n$ if and only if $m = n$.*

Proof. 1. Let V be a finite dimensional F-vector space. Then F has a finite spanning set S and by Theorem 3.43 there is a basis $B \subseteq S$ for V. Thus B is finite and $V = FB$. Set $|B| = n$ and $B = \{b_1, \ldots, b_n\}$. By the UMP for free modules there is linear transformation $f : F^n \to V$ such that $f(e_i) = b_i$ as well as a linear transformation $g : V \to F^n$ such that $g(b_i) = e_i$. Then both $f \circ g : V \to V$ and $g \circ f : F^n \to F^n$ are linear transformation which agree to the identity map on a basis. Hence by the uniqueness part of the UMP for free modules $f \circ g = \mathrm{id}_V$ and $g \circ f = \mathrm{id}_{F^n}$. Therefore these maps are the desired isomorphisms.

2. Let $\varphi : F^m \cong F^n$ be a vector space isomorphism and let B be a basis of F^m.

Claim: $\varphi(B)$ is a basis for F^n. Indeed if $\sum_{i=1}^m c_i \varphi(b_i) = 0$ then $\varphi(\sum_{i=1}^m c_i b_i) = 0$ so $\sum_{i=1}^m c_i b_i = 0$ since φ is injective and $c_i = 0$ fpr all $1 \leq i \leq m$ since B is linearly independent. If $v \in F^n$ then $\phi^{-1}(v) = \sum_{i=1}^m c_i b_i$ since B spans F^m and so $v = \sum_{i=1}^m c_i \varphi(b_i)$, which shows $\varphi(B)$ spans F^n.

By the dimension theorem 3.48, we have $\dim_F(F^n) = n = |\varphi(B)| = |B| = m$. □

Remark 3.51.

1. The same proof as in part 1. above shows that every finitely generated free R-module is isomorphic to R^n for some $n \geq 0$.
2. Part 2. of the classification theorem can be extended to modules over commutative rings as stated in Theorem 3.36.
3. The classification theorem yields that dimension is an isomorphism invariant.

Corollary 3.52. *Two (finite dimensional) vector spaces V, V' over a field F are isomorphic if and only if* $\dim_F(V) = \dim_F(V')$.

February 6 2019
A word on infinite-dimensional vector spaces.

Example. Consider the vector space $F[x]$. This cannot be a finite dimensional vector space. For instance, if $\{f_1, \dots, f_n\}$ were a basis, the element x^{M+1} for $M = \max_{1 \le j \le n}\{\deg(f_j)\}$ would not be in the span of these vectors. We can find a basis for this space though. Consider the collection $B = \{1, x, x^2, \dots\}$. It is clear this set is linearly independent and spans $F[x]$, thus it forms a basis and this basis is *countable*, so $\dim_F F[x] = |\mathbb{N}|$.

Example. Consider the vector space $V = \mathbb{R}^{\mathbb{N}} = \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \dots$. This can be identified with sequences $\{a_n\}$ of real numbers. One might be interested in a basis for this vector space. At first glance the most obvious choice would be $E = \{e_1, e_2, \dots\}$. (It turns out that E is the basis for the direct sum $\bigoplus_{i \in \mathbb{N}} \mathbb{R}$.) However, it is immediate that this set does not span V as $v = (1, 1, \dots)$ can not be represented as a finite linear combination of these elements. Now we know since v is not in $\mathrm{Span}(E)$, that $E \cup \{v\}$ is a linearly independent set. However, it is clear this does not span either as $(1, 2, 3, 4, \dots)$ is not in the span of this set. We know that V has a basis, but it can be shown that no countable collection of vectors forms a basis for this space, in fact $\dim_{\mathbb{R}} \mathbb{R}^{\mathbb{N}} = |\mathbb{R}|$.

We now deduce some formulas that relate the dimensions of various vector spaces.

Theorem 3.53. *Let W be a subspace of a vector space V. Then*

$$\dim(V) = \dim(W) + \dim(V/W).$$

Proof. Homework. □

Remark 3.54. If V, W are both infinite dimensional it can happen that V/W is finite dimensional but also that it is infinite dimensional.

For example, if $V = F[x]$ and $W_1 = (f)$ for some polynomial f with $\deg(f) = d$ then we'll show later that $\dim(F[x]/(f)) = d$. If W_2 is the subspace of all even degree polynomials in $F[x]$ together with the zero polynomial then $\dim(F[x]/W_2) = \infty$.

Example. Consider the vector space $V = \mathbb{R}^2$ and its subspace $W = \mathrm{Span}\{e_1\}$. Then the quotient vector space V/W is, by definition,

$$V/W = \{(x, y) + W \mid (x, y) \in \mathbb{R}^2\}.$$

Looking at each coset we see that

$$(x, y) + W = (x, y) + \mathrm{Span}\{e_1\} = \{(x, y) + (a, 0) \mid a \in \mathbb{R}\} = \{(t, y) \mid t \in \mathbb{R}\},$$

so $(x, y) + W$ is geometrically a line parallel to the x-axis and having the y-intercept y. It is intuitively natural to identify such a line with its intercept, which gives a map

$$V/W \to \text{Span}\{e_2\} \quad (x, y) + W \mapsto (0, y).$$

It turns out that this map is a vector space isomorphism, hence $\dim(V/W) = \dim \text{Span}\{e_2\} = 1$ and we can check that $\dim(W) + \dim(V/W) = 1 + 1 = 2 = \dim(V)$.

Definition 3.55. Let $f : V \to W$ be a linear transformation. The *nullspace* of f is $\text{Ker}(f)$. The *rank* of f is $\dim(\text{Im}(V))$.

Corollary 3.56 (Rank-nullity)**.** *Let $f : V \to W$ be a linear transformation. Then*

$$\dim(\text{Ker}(f)) + \dim(\text{Im}(f)) = \dim(V).$$

Proof. By the first isomorphism theorem for modules we have $V/\text{Ker}(f) \cong \text{Im}(f)$, thus $\dim(V/\text{Ker}(f)) = \dim(\text{Im}(V))$. By the previous theorem we have $\dim(V) = \dim(\text{Ker}(V)) + \dim(V/\text{Ker}(f))$. The desired conclusion follows by substituting the first identity into the second. □

February 8 2019

3.2.2 Linear transformations & homomorphisms between free modules

Lemma 3.57. *If W is a free R-module with basis $C = \{c_1, \ldots, c_m\}$ and $w \in W$ then w can be written* uniquely *as $w = \sum_{j=1}^{m} a_j c_j$ with $a_1, \ldots, a_m \in R$.*

Proof. Exercise. □

Definition 3.58 (The matrix of a homomorphism between free modules)**.** Let R be a commutative ring with $1 \neq 0$. Let V, W, be finitely generated *free* R-modules of rank n and m respectively. Let $B = \{b_1, \ldots, b_n\}$ and $C = \{c_1, \ldots, c_m\}$ be *ordered* bases of V, W. If $f : V \to W$ is an R-module homomorphism then we define elements $a_{ij} \in R$ for $1 \leq i \leq m$ and $1 \leq j \leq n$ by the formulas

$$f(b_i) = \sum_{j=1}^{m} a_{j,i} c_j. \tag{3.2.1}$$

The matrix

$$[f]_B^C = \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{bmatrix}$$

is said to *represent the homomorphism f with respect to the bases B and C.*

Remark 3.59.

- By Lemma, 3.57, the coefficients $a_{j,i}$ in equation 3.2.1 are uniquely determined by the $f(b_i)$ and the elements of C.
- The coefficients $a_{j,i}$ corresponding to $f(b_i)$ form the i-th column of $[f]_B^C$.
- $[f]_B^C \in \mathcal{M}_{m,n}(R)$ i.e. $[f]_B^C$ is an $m \times n$ matrix with entries in R.

Definition 3.60. Let V, W, be finite F-vector spaces of dimension n and m with ordered bases B and C respectively and let $f : V \to W$ be a linear transformation. The matrix $[f]_B^C$ is called the *matrix of the linear transformation* f with respect to the bases B and C.

Example. Let F be a field and consider a linear transformation $f : V \to W$, where $V = F^n$ and $W = F^m$. Consider also the ordered standard bases B and C, i.e. $b_i = e_i \in V$ and $c_i = e_i \in W$. Then for any

$$v = \begin{bmatrix} l_1 \\ \vdots \\ l_n \end{bmatrix} = \sum_i l_i b_i$$

in V we have

$$f(\sum l_i b_i) = \sum_i l_i f(b_i)$$

Each $f(b_i)$ is uniquely expressible as a linear combination of the c_j's as in (3.2.1)

$$f(b_i) = \sum_j a_{j,i} c_j.$$

Then we get

$$f(v) = \sum_i l_i \left(\sum_j a_{j,i} c_j \right) = \sum_j \left(\sum_i a_{j,i} l_i \right) c_j.$$

In other words, we have

$$f(v) = \begin{bmatrix} \sum_i a_{1,i} l_i \\ \vdots \\ \sum_i a_{m,i} l_i \end{bmatrix} = \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{bmatrix} \cdot \begin{bmatrix} l_1 \\ \vdots \\ l_n \end{bmatrix} = [f]_B^C \cdot v.$$

then for any

$$v = \sum_i l_i b_i$$

in V we have and

$$f(\sum l_i b_i) = \sum_i l_i f(b_i)$$

Each $f(b_i)$ is uniquely expressible as a linear combination of the c_j's. Say

$$f(b_i) = \sum_j a_{j,i} c_j.$$

Then we get

$$f(v) = \sum_i l_i \left(\sum_j a_{j,i} c_j \right) = \sum_j \left(\sum_i a_{j,i} l_i \right) c_j.$$

In other words, we have

$$f(v) = [f]_B^C \cdot v$$

where

$$[f]_B^C = \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{bmatrix}$$

and $[f]_B^C \cdot v$ denote the usual rule for matrix multiplication.

This says that any linear transformation $f : F^n \to F^m$ is given by multiplication by a matrix since we noticed above that $f(v) = [f]_B^C \cdot v$. The same type of statement holds for free modules over commutative rings and is given in Proposition 3.61.

Example. Let P_3 denote the the F-vector space of polynomials of degree at most 3 (including the zero polynomial) and consider the linear transformation $d : P_3 \to P_3$ given by $d(f) = f'$, i.e. taking the derivative. Let $B = \{1, x, x^2, x^3\}$. Then

$$[f]_B^B = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Proposition 3.61. *For any commutative ring R with $1 \neq 0$ and finitely generated free R-modules V, W of ranks n and m respectively, fixing ordered bases B for V and C for W gives an isomorphism of R-modules*

$$\mathrm{Hom}_R(V, W) \cong \mathcal{M}_{m,n}(R) \qquad f \mapsto [f]_B^C.$$

If $V = W$ (and thus $m = n$) and $B = C$, then the above map is an R-algebra isomorphism $\mathrm{End}_R(V) \cong \mathrm{M}_n(R)$.

Proof. Let $\varphi : \mathrm{Hom}_R(V, W) \to \mathcal{M}_{m,n}(R)$ be defined by $\varphi(f) = [f]_B^C$. One needs to check that $[f + g]_B^C = [f]_B^C + [g]_B^C$ and $[\lambda f]_B^C = \lambda [f]_B^C$ for any $f, g \in \mathrm{Hom}_R(V, W)$ and $\lambda \in R$. Let $A = [f]_B^C$ and $A' = [g]_B^C$. Then

$$(f + g)(b_i) = f(b_i) + g(b_i) = \sum_j a_{j,i} c_j + \sum_j a'_{j,i} c_j = \sum_j (a_{j,i} + a'_{i,j}) c_j$$

gives $[f+g]_B^C = A + A'$ and

$$(\lambda f)(b_i) = \lambda\left(\sum_j a_{j,i}c_j\right) = \sum_j (\lambda a_{j,i})c_j$$

gives $[\lambda f]_B^C = \lambda A$.

We omit the proof that for $f, g \in \mathrm{End}_R(V)$ we have $[f \circ g]_B^B = [f]_B^B[g]_B^B$.

(For the case where $V = R^n$ this proof would be the following:

$$(f \circ g)(v) = f(g(v)) = f([g]_B^B v) = [f]_B^B([g]_B^B v) = ([f]_B^B[g]_B^B)v,$$

so $[f \circ g]_B^B = [f]_B^B[g]_B^B$.) □

February 11 2019

Corollary 3.62. *For any field F and finite F-vector spaces V, W of dimension n and m respectively,* $\dim \mathrm{Hom}_F(V, W) = mn$.

Proof. The isomorphism $\mathrm{Hom}_F(V, W) \cong \mathcal{M}_{m,n}(F)$ gives

$$\dim_F \mathrm{Hom}_F(V, W) = \dim_F \mathcal{M}_{m,n}(F) = mn.$$

□

3.2.3 Change of basis.

Definition 3.63. Let V be a finitely generated free module over a commutative ring R, and let B and B' be bases of V. Let id_V be the identity map on V. Then $[\mathrm{id}_V]_B^{B'}$ is an invertible matrix called the *change of basis* matrix from B to B'.

In the proof of 3.67 we will show that $[\mathrm{id}_V]_B^{B'}$ is always invertible and its inverse is $\left([\mathrm{id}_V]_B^{B'}\right)^{-1} = [\mathrm{id}_V]_{B'}^B$.

Example. Consider $V = P_2$, let $B = \{1, x, x^2\}$ and $B' = \{1, x-2, (x-2)^2\}$ be bases of V. We calculate the change of basis matrix. We have

$$\begin{aligned}
\mathrm{id}_V(1) &= 1,\\
\mathrm{id}_V(x) &= 2 \cdot 1 + 1 \cdot (x-2),\\
\mathrm{id}_V(x^2) &= 4 \cdot 1 + 4 \cdot (x-2) + 1 \cdot (x-2)^2.
\end{aligned}$$

Thus, the change of basis matrix is given by $[\mathrm{id}_V]_B^{B'} = \begin{bmatrix} 1 & 2 & 4 \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{bmatrix}$.

We now record a general result regarding the matrix representing the composition of two linear transformations, which is a bit more general than that stated at the end of the proof of Proposition 3.61.

Lemma 3.64. *If V, W, U are finitely generated free R-modules spaces with ordered bases B, C, D, and if $f : V \to W$ and $g : W \to U$ are R-module homomorphisms, then*

$$[g \circ f]_D^B = [g]_D^C [f]_C^B.$$

Definition 3.65. Let V be a finitely generated free module over a commutative ring R. Two R-module homomorphisms $f, g : V \to V$ are *similar* if there is a linear transformation $h : V \to V$ such that $g = h \circ f \circ h^{-1}$. Two $n \times n$ matrices A and B with entries in R are *similar* if there is an invertible $n \times n$ matrix P such that $B = PAP^{-1}$.

Remark 3.66. For elements $A, B \in \mathrm{GL}_n(R)$, the notions of similar and conjugate are the same.

Proposition 3.67. *Let V, W be finitely generated free modules over a commutative ring R, let B and B' be bases of V, let C and C' be bases of W, and let $f : V \to W$ be a homomorphism. Then*

$$[f]_{B'}^{C'} = [id_W]_C^{C'} [f]_B^C [id_V]_{B'} B \tag{3.2.2}$$

In particular, if $g : V \to V$ is an R-module homomorphism, then $[g]_B^B$ and $[g]_{B'}^{B'}$ are similar.

Proof. From Lemma 3.64, since $f = \mathrm{id}_W \circ f \circ \mathrm{id}_V$, we have $[f]_{B'}^{C'} = [\mathrm{id}_W]_C^{C'} [f]_B^C [\mathrm{id}_V]_{B'} B$.

Setting $V = W, B = C, B' = C'$ and $f = \mathrm{id}_V$ in (3.2.2) we have $[\mathrm{id}_V]_{B'}^{B'} = [\mathrm{id}_V]_B^{B'} [\mathrm{id}_V]_B^B [\mathrm{id}_V]_{B'}^B$. Notice that $[\mathrm{id}_V]_B^B = [\mathrm{id}_V]_{B'}^{B'} = I$ is the identity matrix, so the previous formula gives $I = [\mathrm{id}_V]_B^{B'} I [\mathrm{id}_V]_{B'}^B$. Setting $P = [\mathrm{id}_V]_B^{B'}$, we notice that the previous identity gives $P^{-1} = [\mathrm{id}_V]_{B'}^B$.

Now set $V = W, B = C, B' = C'$ and $f = g$ in (3.2.2) to obtain

$$[g]_{B'}^{B'} = [\mathrm{id}_V]_B^{B'} [g]_B^B [\mathrm{id}_V]_{B'}^B = P [g]_B^B P^{-1}.$$

□

We now come to special changes of basis and their matrices called elementary matrices:

Definition 3.68. Let R be a commutative ring with $1 \neq 0$, let M be a free R-module of finite rank n, and let $B = \{b_1, \ldots, b_n\}$ be an odered basis for M. An *elementary basis change operation* on the basis B is one of the following three types of operations:

1. Replacing b_i by $b_i + r b_j$ for some $i \neq j$ and some $r \in R$,
2. Replacing b_i by $u b_i$ for some i and some unit u of R,
3. Swapping the indices of b_i and b_j for some $i \neq j$.

Definition 3.69. Let R be a commutative ring with $1 \neq 0$. An *elementary row operation* on a matrix $A \in \mathcal{M}_{m,n}(R)$ is one of the following three types of operations:

1. Adding an element of R times a row of A to a different row of A.
2. Multiplying a row of A by a unit of R.
3. Interchanging two rows of A.

Definition 3.70. Let R be a commutative ring with $1 \neq 0$. An *elementary matrix* over R is an $n \times n$ matrix obtained from I_n by applying a single elementary row operation:

1. For $r \in R$ and $1 \leq i, j \leq n$ with $i \neq j$, let $E_{i,j}(r)$ be the matrix with 1s on the diagonal, r in the (i, j) position, and 0 everywhere else.
2. For $u \in R^\times$ and $1 \leq i \leq n$ let $E_i(u)$ denote the matrix with (i, i) entry u, (j, j) entry 1 for all $j \neq i$, and 0 everywhere else.
3. For $1 \leq i, j \leq n$ with $i \neq j$, let $E_{(i,j)}$ denote the matrix with 1 in the (i, j) and (j, i) positions and in the (l, l) positions for all $l \notin \{i, j\}$, and 0 in all other entries.

Remark 3.71. Let E be an $n \times n$ elementary matrix.

- E is the change of basis matrix $[\mathrm{id}_V]_{B'}^{B}$, where B is any basis of V and B' is the basis obtained from B by the corresponding elementary basis change operation
- If $A \in \mathcal{M}_{n,q}(R)$, then the product matrix EA is the result of performing the corresponding elementary row operation on A.
- If $B \in \mathcal{M}_{m,n}(R)$, then the product matrix BE is the result of performing the corresponding elementary column operation on B.

3.3 Finitely generated modules over PIDs

3.3.1 Presentations for finitely generated modules over Noetherian rings

We studied presentations for groups in the past; these consisted of a set of generators and a set (normal subgroup) of relations among these generators. Presentations are important for modules as well. In this case, the relations are encoded by a matrix, or equivalently by a homomorphism between a pair of free modules. We study below how the change of basis techniques can be applied to unravel the structure of a module starting with its presentation.

Definition 3.72. Let R be a commutative ring with $1 \neq 0$, let $A \in \mathcal{M}_{m,n}(R)$, and let $t_A : R^n \to R^m$ be the R-module homomorphism represented by A with respect to the standard bases (this homomorphism is given by the rule $t_A(v) = Av$). The *R-module presented by A* is the R-module $R^m/\operatorname{Im}(t_A)$.

Example. What $\mathbb{Z}$-module M is presented by

$$A = \begin{bmatrix} 2 & 1 & 0 \\ 3 & 9 & 5 \\ 1 & -2 & 7 \\ 0 & 1 & 2 \end{bmatrix}?$$

Formally, M is the quotient module $M = \mathbb{Z}^4/\operatorname{Im}(t_A)$, where $t_A : \mathbb{Z}^4 \to \mathbb{Z}^3$ is defined by $t_A(v) = Av$. Since $\mathbb{Z}^4$ is generated by its standard basis elements $\{e_1, e_2, e_3, e_4\}$, we deduce as in Lemma 3.28 that $M = \mathbb{Z}^4/\operatorname{Im}(t_A)$ is generated by the cosets of the e_i. To keep the notation short, we set $m_i = e_i + \operatorname{Im}(t_A)$.

Let $N = \operatorname{Im}(t_A)$ and note that N is the submodule of $\mathbb{Z}^4$ generated by the columns of A, i.e.

$$N = R\left\{ \begin{bmatrix} 2 \\ 3 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 9 \\ -2 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 5 \\ 7 \\ 2 \end{bmatrix} \right\} = R\{2e_1 + 3e_2 + e_3, e_1 + 9e_2 - 2e_3 + e_4, 5e_2 + 7e_3 + 2e_4\}.$$

Since N maps to 0 under the quotient map $q : \mathbb{Z}^4 \to M = \mathbb{Z}^4/N$, we have that the relations of M can be written as

$$\begin{cases} 2m_1 + 3m_2 + m_3 & = 0 \\ m_1 + 9m_2 - 2m_3 + m_4 & = 0 \\ 5m_2 + 7m_3 + 2m_4 & = 0. \end{cases}$$

We can now see that this is a rather inefficient presentation, since we can clearly use the first equation to solve for for $m_3 = -2m_1 - 3m_2$. This implies that M can be generated using only m_1, m_2 and m_4, that is

$$M = R\{m_1, m_2, m_3, m_4\} = \{m_1, m_2, m_4\}.$$

This eliminates the first equation and the latter two become

$$\begin{cases} 5m_1 + 15m_2 + m_4 & = 0 \\ -14m_2 - 16m_2 + 2m_4 & = 0 \end{cases}$$

Now we can also eliminate m_4, i.e leaving just two generators m_1, m_2 that satisfy

$$-24m_1 - 46m_2 = 0.$$

Another way to do this is to look at the matrix A and use elementary row operations to "make zeros" on the 1st and 2nd columns as follows:

$$A = \begin{bmatrix} 2 & 1 & 0 \\ 3 & 9 & 5 \\ 1 & -2 & 7 \\ 0 & 1 & 2 \end{bmatrix} \to \begin{bmatrix} 0 & 5 & -14 \\ 0 & 15 & -16 \\ 1 & -2 & 7 \\ 0 & 1 & 2 \end{bmatrix} \to \begin{bmatrix} 0 & 0 & -24 \\ 0 & 0 & -46 \\ 1 & 0 & 13 \\ 0 & 1 & 0 \end{bmatrix}$$

Eliminating the generators m_3 and m_4 amounts to dropping the first two columns (which are the 3rd and 4th standard basis vectors) as well as the last two rows. As we will prove soon, this shows that the $\mathbb{Z}$-module presented by A is isomorphic to the $\mathbb{Z}$-module presented by

$$B = \begin{bmatrix} -24 \\ -46 \end{bmatrix}.$$

We can go further. Set $m_1' := m_1 + 2m_2$. Then m_1' and m_2 also form a generating set of M. The relation on m_1, m_2 translates to

$$-24m_1' + 2m_2 = 0$$

given by the matrix

$$C = E_{1,2}(-2)B = \begin{bmatrix} -24 \\ 2 \end{bmatrix}.$$

Note that we have done a row operation (subtract twice row 1 from row 2) to get from B to C.

Continuing in this fashion by subtracting 12 row 2 from row 1 we also form

$$D = E_{1,2}(12)C = \begin{bmatrix} 0 \\ 2 \end{bmatrix},$$

The last matrix D presents the module $M' = \mathbb{Z}^2/\operatorname{Im}(t_D)$ with generators a, b ($a = e_1 + \operatorname{Im}(t_D), b = e_2 + \operatorname{Im}(t_D)$) and relation $2a = 0$. As we will see, this proves $M \cong \mathbb{Z} \oplus \mathbb{Z}/2$. An explicit isomorphism is given by sending $\mathbb{Z}^2 \to \mathbb{Z} \oplus \mathbb{Z}/2$ by the unique $\mathbb{Z}$-module homomorphism defined by $e_1 \mapsto (1, 0)$ and $e_2 \mapsto (0, [1]_2)$. Now notice that the kernel of this homomorphism is the submodule $(2e_2)\mathbb{Z} = \operatorname{Im}(t_D)$. Then the first isomorphism theorem gives $M' = \mathbb{Z}^2/\operatorname{Im}(t_D) \cong \mathbb{Z} \oplus \mathbb{Z}/2$.

Proposition 3.73. *Let R be a commutative ring with $1 \neq 0$ and let $A \in \mathcal{M}_{m,n}(R)$ and $B \in Mat_{m',n'}(R)$ for some $m, n, m', n' \geq 1$. Then A and B present isomorphic R-modules if and only if B can be obtained from A by any finite sequence of operations of the following form:*

1. *an elementary row operation,*

2. *an elementary column operation,*

3. *deletion of the j-th column and i-th row of A if $Ae_j = e_i$ (that is, if the j-th column of A is the vector e_i),*

4. *the reverse of 3: insertion of a row and column satisfying $Ae_j = e_i$,*

5. *deletion of a column of all 0's,*

6. *the reverse of 5: insertion of a column of all 0's.*

February 15 2019

Proof. Set $M = R^m/\operatorname{Im}(t_A)$ and $M' = R^{m'}/\operatorname{Im}(t_{A'})$, for (1) and (2), where A' is obtained from A by the given elementary row/column operation. We need to prove that there is an isomorphism $M \cong M'$.

1. Since $A' = EA$, the isomorphism $E : R^n \to R^n$ maps $\operatorname{Im}(A)$ bijectively onto $\operatorname{Im}(A')$. Thus Q induces an isomorphism

$$M = R^m/\operatorname{Im}(t_A) \xrightarrow{\cong} R^m/\operatorname{Im}(t_{A'}) = M'.$$

2. Since $A' = AE$ and since E is an isomorphism, we have

$$\operatorname{Im}(t_{A'}) = \operatorname{Im}(t_{AE}) = \operatorname{Im}(t_A \circ t_E) = \operatorname{Im}(t_A)$$

and so $m = m'$ and $M = R^m/\operatorname{Im}(t_A) = R^{m'}/\operatorname{Im}(t_{A'}) = M'$. (For this one we get equality, not merely an isomorphism.)

3. Here $m' = m - 1$ and $n' = n - 1$. Let $p : R^m \twoheadrightarrow R^{m-1}$ be the unique map (guaranteed by the UMP of the free module R^m) sending $e_1, \ldots, e_m$ to $e'_1, \ldots, e'_{i-1}, 0, e'_i, \ldots, e'_{m-1}$, in order, and let $q : R^n \twoheadrightarrow R^{n-1}$ be the map sending $e_1, \ldots, e_n$ to $e'_1, \ldots, e'_{j-1}, 0, e'_j, \ldots, e'_{n-1}$, in order. Here the elements e_i are part of a standard basis for R^n or for R^m, while the elements e'_i are part of a standard basis for R^{n-1} or for R^{m-1}. Then the diagram

$$\begin{array}{ccc} R^n & \xrightarrow{A} & R^m \\ \downarrow{\scriptstyle q} & & \downarrow{\scriptstyle p} \\ R^{n-1} & \xrightarrow{A'} & R^{m-1} \end{array}$$

commutes by the definition of A'. In particular, $p(\operatorname{Im}(t_A)) \subseteq \operatorname{Im}(t_{A'})$ and so p induces an R-module homomorphism

$$\overline{p} : M \to M',$$

and we claim it is bijective.

Since p is onto, so is $\overline{p}$. Suppose $m \in \mathrm{Ker}(\overline{p})$. Then $m = v + \mathrm{Im}(t_A)$ for some $v \in R^m$ and $p(v) \in \mathrm{Im}(t_{A'})$. Say $p(v) = A'w$. Since q is onto, $w = q(u)$ for some u. Then

$$p(v - Au) = p(v) - pA(u) = p(v) - A'q(u) = p(v) - A'w = p(v) - p(v) = 0,$$

and thus $v - Au \in \mathrm{Ker}(p)$. Now, the kernel of p is clearly Re_i, so that $v - Au = re_i$ for some r. Finally, since $Ae_j = e_i$, we have $A(re_j) = re_i = v - Au$ and hence $v = A(u + re_j)$, which proves $v = t_A(u + re_j) \in \mathrm{Im}(t_A)$ and hence that $m = 0$.

5. It is clear that the columns of A' generate the same submodule of R^m as do the columns of A, and thus $M = M'$.

4.& 6. Since the isomorphism relation is reflexive, the statements of parts 3. & 5. show that parts 4.& 6. are true as well.

□

We now address the question of which modules have presentations. It turns out the answer is all, but if we want to make the presentation be finite (that is, so that the matrix describing the module has finitely many rows and columns or equivalently) then we need to restrict ourselves to finitely generated modules. This in general does not suffice to guarantee that there will only be finitely many generators for the submodule of relations, but as we will see, this is indeed the case if we consider modules over a Noetherian ring.

Recall that a commutative ring R is *Noetherian* if R has the ascending chain condition on ideals, as given in Definition 2.82.

Lemma 3.74. *Suppose R is a commutative ring. The following conditions are equivalent:*

1. *R has the ascending chain condition on ideals — i.e., for every chain of ideals*

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

of R there exists an n such that $I_n = I_{n+1} = I_{n+2} = \cdots$.

2. *Every ideal of R is finitely generated — i.e., for every ideal I, there exists a finite set of elements $x_1, \ldots, x_n$ in I such that $I = (x_1, \ldots, x_n)$.*

Proof. Homework. □

Proposition 3.75. *If R is a Noetherian commutative ring, then every submodule of a finitely generated module is again finitely generated.*

It might seem like no submodule of a finitely generated modules could ever fail to itself be finitely generated, but in fact the converse of this Proposition is true too. For observe that R is a module over itself and a submodule of R is exactly the same thing as an ideal. Now observe that R is indeed finitely generated as an R-module — 1 generates R, for example. So, if R is not Noetherian, it has a non-finitely generated ideal I and this represents a submodule of a finitely generated module that fails to be finitely generated.

February 18 2019

Proof of Proposition 3.75. I first prove that for each $n \geq 1$, every submodule of R^n is finitely generated. The base case $n = 1$ holds by definition (since a submodule of R^1 is the same thing as an ideal).

Assume $n > 1$ and the result holds for R^{n-1}. Let M be any submodule of R^n. Define

$$\pi : R^n \twoheadrightarrow R^1$$

to be the projection onto the last component of R^n. The kernel of π_n may be identified with R^{n-1} and so $N := \mathrm{Ker}(\pi) \cap M$ is a submodule of R^{n-1}, and it is therefore finitely generated by assumption. The image $\pi(M)$ of M under π is a submodule of R^1, that is, an ideal of R, and so it too is finitely generated by Lemma 3.74. Furthermore, by the first isomorphism theorem $M/\mathrm{Ker}(\pi) \cong \pi(M)$ is also finitely generated. By Lemma 3.28 part (2.) we deduce that M is a finitely generated module.

I'll just sketch the general case (which I don't think we'll actually need): let T be any finitely generated R-module and $N \subseteq T$ any submodule. Since T is finitely generated, there exists a surjective R-module homomorphism $q : R^n \twoheadrightarrow T$ for some n. Then $q^{-1}(N)$ is a submodule of R^n and hence it is finitely generated by the case we already proved, say by element $v_1, \ldots, v_m \in q^{-1}(N)$. Then it can be shown that $q(v_1), \ldots, q(v_m)$ generate N. □

Proposition 3.76. *Any finitely generated module M over a Noetherian ring R has a finite presentation given by an $m \times n$ matrix A, that is, there is an isomorphism*

$$M \cong R^m/\mathrm{Im}(t_A),$$

where $t_A : R^n \to R^m$ is the map on free modules induced by A, i.e. $t_A(v) = Av$.

Proof. Let M be a finitely generated module over a Noetherian. We start by choosing a finite generating set $y_1, \ldots y_m$ of M. From this we obtain an R-module map

$$\pi : R^m \to M$$

that sends e_i to y_i, by using the UMP for free modules. Since every element in M is (not necessarily uniquely) given as $\sum_{i=1}^m r_i y_i$, the map π is surjective. Let $N = \mathrm{Ker}(\pi)$. Since R^m is finitely generated and R is assumed Noetherian, N is also finitely generated, say by $z_1, \ldots, z_n$. This too leads to a surjective R-module map $g : R^n \twoheadrightarrow N$ that sends

$e_i' \mapsto z_i$. The composition of $g : R^n \twoheadrightarrow N$ followed by the inclusion of $\iota : N \hookleftarrow R^m$ is an R-module homomorphism $t = \iota \circ g : R^n \to R^m$ and hence by Proposition 3.61 t is given by a $m \times n$ matrix $A = [t]_B^C$ with respect to the standard bases of R^m and R^n respectively, i.e. $t = t_A$.

It remains to show that $M \cong R^m / \operatorname{Im}(t_A)$. First note that since $t = \iota \circ g$ and g is surjective we have $\operatorname{Im}(t_A) = \operatorname{Im}(\iota \circ g) = \iota(\operatorname{Im}(g)) = \iota(N) = N = \operatorname{Ker}(\pi)$. By the first isomorphism theorem we now have $M = \operatorname{Im}(\pi) \cong R^m / \operatorname{Ker}(\pi) = R^m / \operatorname{Im}(t_A)$.

□

Remark 3.77. We summarize the situation described in the Proposition above by saying we have an *exact sequence*

$$R^n \xrightarrow{t_A} R^m \xrightarrow{\pi} M \to 0,$$

which means that $\operatorname{Ker}(\pi) = \operatorname{Im}(t_A)$ and also $M \cong \operatorname{Im}(\pi)$. These two conditions imply, as shown above, that $M \cong R^m / \operatorname{Im}(t_A)$.

3.3.2 Classification of finitely generated modules over PIDs

Recall from Lemma 2.83 that any PID R is a Noetherian ring. Hence by Proposition 3.76 any finitely generated R-module M has a finite presentation matrix A. We discuss a canonical form for such a matrix A called the Smith Normal Form and the consequences it has on determining the isomorphism type of M.

Theorem 3.78 (Smith Normal Form (SNF))**.** *Let R be a PID and let $A \in \mathcal{M}_{m,n}(R)$. Then there is a sequence of elementary row and column operations that transform A into a matrix $A' = [a_{ij}']$ such that all non-diagonal entries of A' are 0, and the diagonal entries of A' satisfy*

$$a_{11}' \mid a_{22}' \mid a_{33}' \mid \dots.$$

Moreover, the number j of nonzero entries of A' is uniquely determined by A, and the nonzero diagonal entries $a_{11}', \dots, a_{jj}'$ are unique up to associates.

February 20, 2019

Example. If A is a 1×2 matrix, the existence portion of the Lemma amounts to the Euclidean algorithm: Given (x, y), by subtracting a multiple of the one entry to the other in the usual back-and-forth way, we arrive at $(\gcd(x, y), 0)$.

The proof in general amounts to a sort of extended Euclidean algorithm.

Proof. To prove existence, we claim there is a sequence of row and column operations that transforms A to

$$\begin{bmatrix} g & 0 \\ 0 & B \end{bmatrix}$$

for some $(n-1) \times (m-1)$ matrix B and where $g = \gcd(A)$. (We adopt the convention that if A is the matrix of all 0's, then $g = 0$.) Granting this, we are done: For notice

that g divides every entry of B, and so by applying this fact over and over again we arrive at a matrix of the desired form A'.

Let a be the upper-left entry of A. Suppose a happens to be $g = \gcd(A)$. Then, in particular, it divides every entry of the first row and column of A, and so by doing row and column operations, we may 0 out these entries to arrive at a matrix of the desired form directly.

We proceed by inducution on the number of prime factors of a/g. If there are no prime factors, then $a = \gcd(A)$, and we already did this case. Otherwise, there is at least one entry $b = a_{i,j}$ such that $a \nmid b$. If we can find such a b belonging to the first row of A, then we may implement the Euclidean algorithm in the form of suitable column operations, to replace a by $\gcd(a, b)$ (and b by 0). Since $\gcd(a, b)/g$ has fewer prime factors than a/g, we are done by induction. Likewise if there exists such a b in the first column, we are done by induction.

The remaining possibility is that a divides every entry of the first row and first column. In this case, as before we can 0 them out by row and column operations to obtain a matrix of the form

$$C = \begin{bmatrix} a & 0 \\ 0 & E \end{bmatrix}.$$

Since $\gcd(C) = \gcd(A)$, there is some element e of E such that $a \nmid e$. A suitable row operation puts e into row one without affecting a. We have thus reduced the problem to a previously solved case.

We prove uniqueness next, but our proof will be a bit sketchy.

Since R is a PID, the gcd of any collection of elements of R is any one of the principal generators of the ideal generated by the collection.

For any i and any matrix B, let $\gcd_i(B)$ denote the gcd of all the $i \times i$ minors of B. We will not prove this, but it is true and not hard to see that, for any i and any commutative ring, the ideal generated by the $i \times i$ minors of a matrix is unchanged by row and column operations. It follows that for a PID, $\gcd_i$ is unchanged by row and column operations.

For a matrix of the form A', the only minors that are non-zero are those involving the same choices of columns and rows, and hence the only non-zero $i \times i$ minors of A' are $g_{s_1} \cdots g_{s_i}$ for some $s_1 < \cdots < s_i$. Since the g_s's divide each other, it follows that

$$\gcd_i(A) = \gcd_i(A') = g_1 \cdots g_i.$$

In paticular, the largest value of i such that some $i \times i$ minor of A is non-zero is j. Also, we have

$$g_i = \frac{\gcd_i(A)}{\gcd_{i-1}(A)}.$$

This proves uniqueness, for it shows that $j, g_1, \ldots, g_j$ are all defined from A directly, without any choices. □

February 25 2019

We now proceed to classify modules over PIDs using the SNF for their presentation matrix. First a lemma on how to interpret the module presented by a matrix in SNF.

Lemma 3.79. *Let R be a commutative ring with $1 \neq 0$, let $m \geq n$, let $A = [a_{ij}] \in \mathcal{M}_{m,n}(R)$ be a matrix such that all non-diagonal entries of A are 0, and let M be the R-module presented by A. Then $M \cong R^{m-n} \oplus R/(a_{11}) \oplus \cdots \oplus R/(a_{nn})$.*

Proof. HW. □

Theorem 3.80 (Classification of finitely generated modules over a PID using invariant factors(CFGMPIDIF))**.** *Let R be a PID and let M be a finitely generated module. Then there exist $r \geq 0, k \geq 0$, and nonzero non unit elements $d_1, \ldots, d_k$ of R satisfying $d_1 \mid d_2 \mid \cdots \mid d_k$ such that*

$$M \cong R^r \oplus R/(d_1) \oplus \cdots \oplus R/(d_k).$$

Moreover r and k are uniquely determined by M, and the d_i are unique up to associates.

Definition 3.81. Let R be a PID, let $r \geq 0, k \geq 0$, and let $d_1, \ldots, d_k$ be nonzero non unit elements of R satisfying $d_1 \mid d_2 \mid \cdots \mid d_k$. Let M be any R-module such that $M \cong R^r \oplus R/(d_1) \oplus \cdots \oplus R/(d_k)$. The *free rank* of M is the integer r. The elements $d_1, \ldots, d_k$ are the invariant factors of M.

Proof. By Proposition 3.76, M has a presentation matrix A and by Theorem 3.78 this matrix can be put into Smith Normal Form A', where the diagonal entries of A' are $d_1, \ldots, d_k$ and satisfy $d_1 \mid d_2 \mid \cdots \mid d_k$. Moreover k is unique and the d_i's are uniquely determined up to associates by A, hence by M. By Proposition 3.76, M is isomorphic to the module presented by A' and by the previous Lemma, this is isomorphic to $M \cong R^r \oplus R/(d_1) \oplus \cdots \oplus R/(d_k)$. □

Remark 3.82. The theorem can be interpreted as saying that M decomposes into a free submodule R^r and a torsion submodule $\mathrm{Tor}(M) = R/(d_1) \oplus \cdots \oplus R/(d_k)$. (The latter equality is to be proven on homework.)

Example. Consider the $\mathbb{Z}$-module M presented by the matrix $A = \begin{bmatrix} 1 & 6 & 5 & 2 \\ 2 & 1 & -1 & 0 \\ 3 & 0 & 3 & 0 \end{bmatrix}$. As shown on HW, the Smith normal form of A is $A' = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 6 & 0 \end{bmatrix}$, with invariant factor $d_1 = 6$ (note that the invariant factors must be non units). Therefore we have $M \cong \mathbb{Z}/(1) \oplus \mathbb{Z}/(1) \oplus \mathbb{Z}/(6) \cong \mathbb{Z}/(6)$.

Corollary 3.83 (FTFGAG – invariant factor form)**.** *Let G be a finitely generated abelian group. Then $G \cong \mathbb{Z}^r \oplus (\mathbb{Z}/n_1) \oplus \cdots \oplus (\mathbb{Z}/n_k)$ for some $r \geq 0, k \geq 0$, and $n_i \geq 2$ for all i, satisfying $n_{i+1} \mid n_i$ for all i. Moreover, the integers $r, k, n_1, \ldots, n_k$ are uniquely determined by G.*

Here is a spinoff of the CFGMPIDIF.

Theorem 3.84 (Classification of finitely generated modules over a PID using elementary divisors (CFGMPIDED)). *Let R be a PID and let M be a finitely generated module. Then there exist $r \geq 0, k \geq 0$, prime elements $p_1, \ldots, p_s$ of R (not necessarily distinct), and $e_1, \ldots, e_s \geq 1$, such that*

$$M \cong R^r \oplus R/(p_1^{e_1}) \oplus \oplus R/(p_s^{e_s}).$$

Moreover r and k are uniquely determined by M, and the list $p_1^{e_1}, \ldots, p_s^{e_s}$ is unique up to associates and reordering.

Proof. First write M in invariant factor form $M \cong R^r \oplus R/(d_1) \oplus \cdots \oplus R/(d_k)$ then write each invariant factor as a product of prime powers $d_i = \prod_{j=n_i}^{n_{i+1}} p_j^{e_j}$ and recall that by the Chinese remainder theorem we have $R/(d_i) \cong R/(p_{n_i}^{e_{n_i}}) \oplus \cdots \oplus R/(p_{n_{i+1}}^{e_{n_{i+1}}})$. Substituting this into the invariant factor form gives the desired result. Uniqueness follows from the uniqueness of the invariant factor form and of the prime factorizations of the d_i's. □

Definition 3.85. Let R be a PID, let $r \geq 0, s \geq 0$, let $p_1, \ldots, p_s$ be prime elements of R, and let $e_1, \ldots, e_s \geq 1$. Let M be the R-module $M \cong R^r \oplus R/(p_1^{e_1}) \oplus \cdots \oplus R/(p_s^{e_s})$. The elements $p_1^{e_1}, \ldots, p_s^{e_s}$ of R are the *elementary divisors* of M.

Example. Continuing with $M \cong \mathbb{Z}/(6)$ from the previous example, we have $M \cong \mathbb{Z}/(6) \cong \mathbb{Z}/(2) \oplus \mathbb{Z}/(3)$, so the elementary divisors are 2 and 3.

Corollary 3.86 (FTFGAG–elementary divisors form). *Let G be a finitely generated abelian group. Then there exist $r, s \geq 0$ prime integers $p_1, \ldots, p_s$ and positive integers $e_i \geq 1$ such that $G \cong \mathbb{Z}^r \oplus \mathbb{Z}/p_1^{e_1} \oplus \cdots \oplus \mathbb{Z}/p_s^{e_s}$. Moreover, the r, p_i's, and e_i's are uniquely determined by G.*

Cutoff point for midterm.

3.4 Canonical forms for endomorphisms

3.4.1 Rational canonical form (RCF)

Recall that given an F-vector space V with $\dim_F(V) = n$ and an ordered basis B for V we have proven in Proposition 3.61 that $\mathrm{End}_F(V) \cong \mathrm{M}_n(F)$ via the maps $t \mapsto [t]_B^B$ and $A \mapsto t_A$.

Recall also from Proposition 3.18:

Definition 3.87. Let F be a field, let V be a finite dimensional vector space over F, and let $t : V \to V$ be a linear transformation. The $F[x]$-module V_t is defined to be the vector space V with the unique $F[x]$-action satisfying $xv = t(v)$ for all $v \in V$. That is,

$$(r_n x^n + \cdots + r_0)v = r^n t^n(v) + \cdots + r_0 v \text{ for all } r_n x^n + \cdots + r_0 \in F[x].$$

Theorem 3.88. *Let F be a field, let V be an F-vector space of dimension n, let $t : V \to V$ be a linear transformation, let B be an ordered basis for V, and let $A = [t]_B^B$. Then the matrix $xI_n - A \in \mathcal{M}_n(F[x])$ presents the $F[x]$-module V_t.*

February 27, 2019

Proof. Let $B = \{b_1, \ldots, b_n\}$ be any basis for V_t. For the free $F[x]$-module $F[x]^n$, let $e_1, \ldots, e_n$ denote its standard $F[x]$-basis. Let $\pi : F[x]^n \to V_t$ be the surjective $F[x]$-module homomorphism sending e_i to b_i. That is,

$$\pi((g_1(x), \ldots, g_n(x)) = \pi(\sum_{i=1}^{n} g_i(x)e_i) = \sum_{i=1}^{n} g_i(x)b_i = \sum_{i=1}^{n} g_i(t)b_i.$$

By the first isomorphism we have $V_t \cong F[x]^n/\operatorname{Ker}(\pi)$. Note that $xI_n - A$ determines a map

$$t_{xI_n - A} : F[x]^n \to F[x]^n,$$

and to show that $F_t \cong F[x]^n/\operatorname{Im}(t_{xI_n-A})$ it suffices to show that $\operatorname{Im}(t_{xI_n-A}) = \operatorname{Ker}(\pi)$.

The composition $\pi \circ t_{xI_n-A}$ sends

$$(\pi \circ t_{xI_n-A})(e_i) = \pi((xI_n - A)e_i) = (xI_n - A)\pi(e_i) = (xI_n - A)b_i = xb_i - Ab_i = t(b_i) - t(b_i) = 0$$

by definition of how x acts on F_A^n. This proves $\operatorname{Im}(xI_n - a) \subseteq \operatorname{Ker}(\pi)$. It follows by the UMP of quotient modules that there is a surjection of $F[x]$-modules

$$W := F[x]^n/\operatorname{Im}(xI_n - A) \twoheadrightarrow V_t.$$

We may also regard this as a surjection of F-vector spaces. Since $\dim_F(V_t) = n$ and the map above is surjective, we have $\dim_F(W) \geq n$ and to establish that the map above is an isomorphism it suffices to prove that $\dim_F(W) \leq n$.

Denote by $\tilde{e}_i = e_i + \operatorname{Im}(xI_n - A)$ the image of the standard basis of $F[x]^n$ in W. The i-th column of $xI_n - A$ gives the relation $x\tilde{e}_i = v_i$ in W, where v_i is the i-th column of A. It follows that $p(x)\tilde{e}_i = p(A)\tilde{e}_i$ in W for any polynomial $p(x)$. Thus a typical element of W, given by $\sum_i g_i(x)\tilde{e}_i$, is equal to $g_1(A)\tilde{e}_1 + \cdots + g_n(A)\tilde{e}_n$. Such an expression belongs to the F-span of $\tilde{e}_1, \ldots, \tilde{e}_n$ in W; that is; $\tilde{e}_1, \ldots, \tilde{e}_n$ span W as an F-vector space and consequently we have the desired inequality $\dim_F(W) \leq n$. □

Corollary 3.89. *Suppose F is a field, V is an F-vector space and and $t : V \to V$ is a linear transformation. Then there exist unique monic polynomials $g_1, \ldots, g_k \in F[x]$ of positive degree such that $g_i | g_{i+1}$ for all i and there is an $F[x]$-module isomorphism*

$$V_t \cong F[x]/(g_1) \oplus \cdots \oplus F[x]/(g_k).$$

The polynomials $g_1, \ldots, g_k$ are the invariant factors of the $F[x]$-module V_t and the entries on the diagonal of the Smith normal form of $xI_n - [t]_B^B$ for any basis B of V.

Proof. Follows from the FTFGMPIDIF and the previous proposition. □

Definition 3.90. The polynomials $g_1, \ldots, g_k$ in the previous Corollary are called the *invariant factors* of the linear transformation t_A.

Example. Let $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in \mathrm{M}_2(\mathbb{Q})$. Then $xI_2 - A = \begin{bmatrix} x-1 & -1 \\ 0 & x-1 \end{bmatrix}$. We could compute the invariant factors of $t_A : \mathbb{Q}^2 \to \mathbb{Q}^2$ by appealing to the SNF of $xI_2 - A$, but let's try another way. Call d_1, d_2 the entries on the diagonal of the SNF of $xI_2 - A$. Recall from the proof of 3.78 that d_1 is the gcd of the entries of $xI_2 - A$ and $d_1 d_2 = \det(xI_2 - A)$. Thus $d_1 = 1$ and $d_2 = \det(xI_2 - A) = (x-1)^2$. Therefore the only invariant factor of t_A is $(x-1)^2$.

The previous Corollary gives us Rational Canonical Form of the matrix A. This follows from the Lemma:

Lemma 3.91. *For a monic polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0$ with $n \geq 1$, the elements $1, x, \ldots, x^{n-1}$ form a basis for $F[x]/(f(x))$ regarded as an F-vector space. Relative to this basis, the F-linear operator $l_x : F[x]/(f(x)) \to F[x]/(f(x))$ defined by $l_x(v) = xv$ is given by the following matrix,*

$$C(f) := \begin{bmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \ddots & 0 & -a_2 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & 1 & -a_{n-1} \end{bmatrix}$$

Proof. HW □

Definition 3.92. In the setup of Lemma 3.91, the matrix $C(f)$ is called the *companion matrix* of the monic polynomial f.

Definition 3.93. Let F be a field and let $A \in \mathcal{M}_m(F)$ and $B \in \mathcal{M}_n(F)$. The matrix $A \oplus B$ is the matrix $[c_{ij}] \in \mathrm{M}_{m+n}(F)$ defined by $c_{ij} = a_{ij}$ for all $1 \leq i, j \leq m$, $c_{ij} = b_{i-m,j-m}$ for all $m+1 \leq i, j \leq m+n$, and $c_{ij} = 0$ otherwise. This is to say

$$A \oplus B = \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}.$$

Remark 3.94. If $f : V_1 \to W_1$ and $g : V_2 \to W_2$ are linear transformations then the map $f \oplus g : V_1 \oplus V_2 \to W_1 \oplus W_2$ given by $(f \oplus g)(a, c) = (f(a), g(c))$ is a linear transformation and if B_i is a basis for V_i and C_i is a basis for W_i then $\mathcal{B} = \iota_1(B_1) \cup \iota_2(B_2)$ is a basis for $V_1 \oplus V_2$, $\mathcal{C} = \iota_1(C_1) \cup \iota_2(C_2)$ is a basis for $W_1 \oplus W_2$ and

$$[f \oplus g]^{\mathcal{C}}_{\mathcal{B}} = \begin{bmatrix} [f]^{C_1}_{B_1} & 0 \\ 0 & [g]^{C_2}_{B_2} \end{bmatrix}.$$

Theorem 3.95. *Suppose F is a field, V is a finite dimensional F-vector space, and $t : V \to V$ is an F-linear transformation. There is a basis B of V such that*

$$[t]_B^B = C(g_1) \oplus \cdots \oplus C(g_l) = \begin{bmatrix} C(g_1) & 0 & 0 & \cdots & 0 \\ 0 & C(g_2) & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & & \vdots \\ 0 & 0 & \cdots & 0 & C(g_k) \end{bmatrix}$$

where $g_1, \ldots, g_l$ are the invariant factors of t, i.e. they are monic polynomials of positive degree such that $g_1 \mid g_2 \mid \cdots \mid g_k$. Moreover, $g_1, \ldots, g_k$ are unique.

Proof. We know by Corollary 3.89 that $V_t \cong \bigoplus_{i=1}^k F[x]/(g_i(x))$ for unique g_i's as in the statement. Set $V_i = F[x]/(g_i(x))$ and note that $V_t = V_1 \oplus \cdots \oplus V_k$. Multiplication by x, $l_x : V_t \to V_t$ preserves each summand in this decomposition, i.e. $l_x(V_i) \subseteq V_i$ and so if we choose a basis B_i of each summand V_i and set $B = \bigcup_{i=1}^k \iota_i(B_i)$, then by the previous Remark, B is a basis of V_t and $[t]_B^B = [t|_{V_1}]_{B_1}^{B_1} \oplus \cdots \oplus [t|_{V_k}]_{B_k}^{B_k}$. So the result follows from Lemma 3.91. □

Definition 3.96. In the setup of Theorem 3.95, the matrix $C(g_1) \oplus \cdots \oplus C(g_l)$ is called the *rational canonical form* (RCF) of the linear transformation t. By extension, given a matrix $A \in \mathrm{M}_n(F)$, the rational canonical form of that matrix is defined to be the rational canonical form of the endomorphism t_A represented by A with respect to the standard basis of F^n.

Example. Let $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in \mathrm{M}_2(\mathbb{Q})$ as in Example 3.4.1. Because the only invariant factor of t_A is $(x-1)^2$, the RCF of t_A is

$$RCF(A) = C((x-1)^2) = C(x^2 - 2x + 1) = \begin{bmatrix} 0 & -1 \\ 1 & 2 \end{bmatrix}.$$

3.4.2 Characteristic polynomial, minimal polynomial, Cayley-Hamilton

Definition 3.97. Let F be a field and let $A \in \mathcal{M}_n(F)$. The *characteristic polynomial* of A is the polynomial $c_A = \det(xIn - A)$.

Definition 3.98. Let V be an F-vector space of dimension n, and let $t : V \to V$ be a linear transformation. The *characteristic polynomial* of t, denoted c_t, is the polynomial c_A for a matrix $A = [t]_B^B$ with respect to some ordered basis B of V.

Remark 3.99.
- The characteristic polynomial c_t of t is well-defined since similar matrices have the same characteristic polynomial.

- For any matrices A, B, $c_{A\oplus B} = c_A c_B$.

Definition 3.100. Let F be a field and let $A \in \mathcal{M}_n(F)$. The *minimal polynomial* of A, denoted m_A, is a monic polynomial of least degree such that $m_A(A) = 0$.

Definition 3.101. Let V be an F-vector space of dimension n, and let $t : V \to V$ be a linear transformation. The *minimal polynomial* of t, denoted m_t, is the monic polynomial generating the annihilator ideal $\mathrm{Ann}_{F[x]}(V_t)$ in the PID $F[x]$.

Remark 3.102. If $m(x)$ is the minimal polynomial of a matrix A or of an endomorphism t and $f(x)$ is another polynomials such that $f(A) = 0$ or $f(x)$ annihilates V_t respectively, then $m(x) \mid f(x)$.

Lemma 3.103. *Let F be a field. Let V be an F-vector space of dimension n with basis B and let $t : V \to V$ be a linear transformation. The minimal polynomial m_A of $A = [t]_B^B$ satisfies $m_A = m_t$.*

Proof. We need to show that $\mathrm{Ann}_{F[x]}(V_t) = (m_A)$. Indeed,

$$\begin{aligned} f \in \mathrm{Ann}_{F[x]}(V_t) &\iff f(x)v = 0 \forall v \in V_t \\ &\iff f(A)v = 0 \forall v \in V_t \\ &\iff \mathrm{Ker}(f(A)) = V_t \\ &\iff \mathrm{rank}(f(A)) = 0 \\ &\iff f(A) = 0 \\ &\iff m_A(x) \mid f(x) \\ &\iff f \in (m_A). \end{aligned}$$

□

Remark 3.104. For any polynomial $f \in F[x]$, we have $m_{C(f)} = c_{C(f)} = f$. The statement $m_{C(f)} = f$ follows because $C(f)$ represents the endomorphism of the vector space $F[x]/(f(x))$ given by multiplication by x and the annihilator of this $F[x]$-module is $(f(x))$. In particular this yields $\deg(m_{C(f)}) = \deg(f)$. The equality $m_{C(f)} = c_{C(f)}$ follows since $m_{C(f)} \mid c_{C(f)}$ and $\deg(m_{C(f)}) = \deg(f) = \deg(c_{C(f)})$ and $m_{C(f)}, c_{C(f)}$ are both monic polynomials.

Definition 3.105. Let V be a vector space over a field F. Let $t : V \to V$ be a linear transformation. A nonzero element $v \in V$ satisfying $t(v) = \lambda v$ for some $\lambda \in F$ is an *eigenvector* of t with *eigenvalue* λ. Let $A \in \mathcal{M}_n(F)$. A nonzero element $v \in F^n$ satisfying $Av = \lambda v$ for some $\lambda \in F$ is an *eigenvector* of A with eigenvalue λ.

Remark 3.106. The scalar $\lambda \in F$ is an eigenvalue of A if and only if it is a root of the characteristic polynomial $c_A(x) = \det(xI_n - A)$, i.e. $c_A(\lambda) = 0$.

March 4, 2019

Theorem 3.107. *Let F be a field, let V be a finite dimensional F-vector space, and let $t : V \to V$ be a linear transformation with invariant factors $g_1, \ldots, g_k$ with $g_i | g_{i+1}$ for all i.*

1. $c_t = g_1 \ldots g_k$.
2. $m_t = g_k$.
3. *(Cayley-Hamilton Theorem):* $m_t \mid c_t$, *and hence* $c_t(t) = 0$.
4. $c_t \mid m_t^k$.
5. *Let $f \in F$. The following are equivalent:*
   (a) *λ is an eigenvalue of t.*
   (b) *λ is a root of c_t.*
   (c) *λ is a root of m_t.*

Proof. (1.) Since c_t is invariant under base change, we have

$$c_t = c(C(g_1) \oplus \cdots \oplus C(g_k)) = c_{(C(g_1))} \cdot \cdots \cdot c_{(C(g_k))} = g_1 \cdots g_k.$$

(2.) From the homework, $\mathrm{Ann}_{F[x]}(v_t) = (g_k)$ and since g_k is monic we deduce that $m_t = g_k$.
(3.) Follows from (1.) and (2.)
(4.) Follows since $g_i \mid g_k$ for $1 \leq i \leq k$, hence $c_t = g_1 \ldots g_k \mid g_k^k = m_t^k$.
(5.) $(a) \iff (b)$ is well known and $(b) \iff (c)$ follows from (3.) and (4.) □

Example. Let's find the minimal and characteristic polynomials of $T : \mathbb{R}^2 \to \mathbb{R}^2$ given as rotation by 60 degrees counter-clockwise. We could write this down as matrix and compute its characteristic polynomial, but a simpler way it so notice that $T^3 = -I_2$ and so T satisfies the polynomial $x^3 + 1 = (x + 1)(x^2 - x + 1)$. It minimal polynomial must therefore divide x^3+1 and so it must either be $x+1$ or x^2-x+1 (since the latter is irreducible in $\mathbb{R}[x]$). It is were $x+1$ then T would be $-I_2$ which is clearly incorrect. So the minimal polynomial is x^2-x+1. By Cayley-Hamilton, this polynomial must divide the characteristic polynomial and since the latter also has degree two, we conclude

$$c_T(x) = x^2 - x + 1.$$

This this is irreducible, there is in this example no choice for how to form the invariant factors: there must just be one of them, $c_T(x)$ itself. So

$$C(x^2 - 1 + 1) = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}$$

is the rational canonical form of T.

Theorem 3.108. *Let F be a field and let $A, A' \in \mathcal{M}_n(F)$. The following are equivalent.*

1. *A and A' are similar matrices.*
2. *A and A' have the same RCF.*
3. *A and A' have the same invariant factors.*

Proof. (1.) $\Rightarrow$ (2.) follows because, if A is similar to A', then the matrices $xI_n - A$ and $xI_n - A'$ are also similar and similar matrices have the same Smith normal form.

(2.) $\Rightarrow$ (3.) follows because the invariant factors can be read off the RCF.

(3.) $\Rightarrow$ (1.) follows because if A and A' have the same invariant factors then there is an isomorphism of $F[x]$-modules $F^n_{t_A} \cong F^n_{t_{A'}}$, which implies by a homework problem that A and A' must be similar. $\square$

3.4.3 Jordan canonical form (JCF)

We now turn toward Jordan canonical form. To motivate it, let us do an example.

Example. Let us consider

$$A = \begin{bmatrix} 0 & 0 & 8 \\ 1 & 0 & -12 \\ 0 & 0 & 6 \end{bmatrix} = C((x-2)^3) \in \mathrm{M}_3(\mathbb{Q}).$$

This means we can interpret this matrix as arising from the linear transformation l_x on

$$V = \mathbb{Q}[x]/(x-2)^3$$

given by multiplication by x. Recall that the basis that gives the matrix A is

$$B = \{\overline{1}, \overline{x}, \overline{x^2}\}$$

But notice that

$$B' = \{\overline{(x-2)^2}, \overline{x-2}, \overline{1}\}$$

is also a basis of V and indeed seems like a more pleasing one. Let us calculate what the operator T does to this alternative basis. We could work this out by brute force, but a cleaner way is to first compute what the operator $T' = T - 2\mathrm{id}_V$ does. It is clear that T' is multiplication by $x-2$ and hence T' sends each basis element to the previous one, except for the first which is sent to 0. That is the matrix of T' is

$$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}$$

and hence the matrix for T is $T' + 2I_3$:

$$J_3(2) := \begin{bmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{bmatrix}$$

This is a *Jordan Block*.

Definition 3.109. Let F be a field, let $n > 0$, and let $r \in F$. The *Jordan block* $J_n(r)$ is the $n \times n$ matrix over F with entries a_{ij} (in row i column j) satisfying $a_{ii} = r$ for all $1 \leq i \leq n$, $a_{i,i+1} = 1$ for all $1 \leq i \leq n-1$, and $a_{ij} = 0$ for all other i, j.

March 6, 2019

Theorem 3.110 (Jordan Canonical Form Theorem)**.** *Let F be a field, let V be a finite dimensional vector space, and let $t : V \to V$ be a linear transformation satisfying the property that the characteristic polynomial c_t of t factors completely into linear factors. Then there is an ordered basis B for V such that*

$$[t]_B^B = J_{e_1}(r_1) \oplus \cdots \oplus J_{e_s}(r_s) = \begin{bmatrix} J_{e_1}(r_1) & 0 & 0 & \cdots & 0 \\ 0 & J_{e_2}(r_2) & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & & \vdots \\ 0 & 0 & \cdots & 0 & J_{e_s}(r_s) \end{bmatrix}$$

such that each $r_i \in F$ is a root of c_t and each $e_i \geq 1$. Moreover, the polynomials $(x - r_1)^{e_1}, \ldots, (x - r_s)e^s$ are the elementary divisors of the $F[x]$-module V_t, and this expression for $[t]_B^B$ is unique up to ordering of the Jordan blocks.

Proof. The proof is along the lines of the previous example. First write V_t in terms of the elementary divisors as follows

$$V_t \cong F[x]/((x - r_1)^{e_1}) \oplus \cdots \oplus F[x]/((x - r_s)^{e_s}).$$

Then pick bases $B_i' = \{\overline{(x - r_i)^{e_i - 1}}, \ldots, \overline{x - r_i}, \overline{1}\}$ for each of the summands and set $B = \bigcup_{i=1}^s \iota_i(B_i')$. By the same argument as in the example applied to each summand individually, the matrix representing multiplication by x on each summand is $J_{e_i}(r_i)$. □

Definition 3.111. Let F be a field, let V be a finite dimensional vector space, and let $t : V \to V$ be a linear transformation satisfying the property that the characteristic polynomial c_t of t factors completely into linear factors and has with elementary divisors $(x - r_1)^{e_1}, \ldots, (x - r_s)^{e_s}$. The matrix $J_{e_1}(r_1) \oplus \cdots \oplus J_{e_s}(r_s)$ is a *Jordan canonical form* (JCF) of t.

Let $A \in \mathcal{M}_n(F)$ and let $t : F^n \to F^n$ be the linear transformation such that $A = [t]_E^E$, where E is the standard basis of F^n. A Jordan canonical form (JCF) of A is a Jordan canonical form of t_A.

The same matrix may fail to have a JCF when interpreted as a matrix with entries in a smaller field while it has a JCF when interpreted as a matrix with entries in a larger field.

Example. We revisit the example of the rotation by 60° but extend scalars to $\mathbb{C}$. That is, start with a matrix A with $c_A(x) = x^2 - x + 1 = (x - w)(x - \overline{w})$ where $w = \frac{1+\sqrt{3}i}{2}$. Since the minimal polynomial $m_A = x^2 - x + 1$ as well we deduce that the only invariant factor of A is $x^2 - x + 1$ and hence the RCF of A is $C(x^2 - x + 1)$. On the other hand, by the Chinese Remainder Theorem

$$\mathbb{C}[x]/(x^2 - x + 1) \cong \mathbb{C}[x]/(x - w) \oplus \mathbb{C}[x]/(x - \overline{w})$$

and so

$$A \sim C(x - w) \oplus C(x - \overline{w}) = \begin{bmatrix} w & 0 \\ 0 & \overline{w} \end{bmatrix}$$

and the latter matrix is the JCF of A (and in this case the JCF is a diagonal matrix). Notice that if we consider $A \in \mathrm{M}_2(\mathbb{R})$ then the characteristic polynomials fails to factor into linear factors. Hence $A \in \mathrm{M}_2(\mathbb{R})$ does not have a JCF.

Definition 3.112. Let F be a field, let V be a finite dimensional vector space, and let $t : V \to V$ be a linear transformation. Then t is *diagonalizable* if there is a basis B for V such that the matrix $[t]_B^B$ is a diagonal matrix. Let $A \in \mathcal{M}_n(F)$. Then A is *diagonalizable* if A is similar to a diagonal matrix.

Theorem 3.113. *Let F be a field, let V be a finite dimensional vector space, and let $t : V \to V$ be a linear transformation. The following are equivalent:*

1. *t is diagonalizable.*
2. *t has a Jordan canonical form A and A is a diagonal matrix.*
3. *t has a Jordan canonical form and the elementary divisors are all of the form $(x - r)^1$ (with $r \in F$).*
4. *Each invariant factor of t is a product of linear polynomials with no repeated linear factors.*
5. *The minimal polynomial of t is a product of linear polynomials with no repeated linear factors.*

Proof. Note that a diagonal matrix is an example of a matrix in JCF. So (1) holds if and only if (2) holds, by the uniqueness of JCF. (2) holds if and only if (3) holds by definition. A matrix has a JCF if and only if its invariant factors factor completely. In this case, the elementary divisors are constructed by decomposing each invariant factor into powers of distinct linear polynomials. This gives that (3) holds if and only if (4) holds. (4) holds if and only if (5) holds, since the minimal polynomial is one of the invariant factors and every other invariant factor divides it. □

Chapter 4

Field Extensions and Galois Theory

4.1 Field extensions

4.1.1 Definition and first properties

One motivation for studying field extensions is that we want to build fields in which certain polynomials have roots.

A classical example (which goes back to Gauss) is that, if we want a field in which the polynomial $x^2 + 1 \in \mathbb{R}[x]$ has a root we obtain $\mathbb{C} = \mathbb{R}(i) = \{a + bi \mid a, b \in \mathbb{R}\}$.

Another example, from last time, is the polynomial $x^2 - x + 1$. Let's think about it as being in $\mathbb{Q}[x]$. We know that this has a root $\omega = \frac{1+\sqrt{3}i}{2} \in \mathbb{C}$. But if we look for the smallest field in which x^2-x+1 has a root we obtain the field $\mathbb{Q}(\omega) = \{a+b\omega \mid a, b \in \mathbb{Q}\}$.

So, one way to build a larger field L from a smaller field F and a polynomial $f \in F[x]$ is to take a root α of that polynomial and adjoin it to F obtaining $L = F(\alpha)$ as the collection of all expressions that one can build using addition, subtraction, multiplication and division starting from the of elements of $F \cup \{\alpha\}$.

Another way to build a larger field L from a smaller field F and an irreducible polynomial $f \in F[x]$ is to let $L = F[x]/(f(x))$. We will show below that these two ways of creating larger fields are one and the same.

Definition 4.1. A *field extension* is an inclusion of one field F into a larger field L, making F into a subfield of L. I sometimes will write $F \subseteq L$ and sometimes L/F to signify that L is a field extension of F.

So a field extension is just another name for a subfield, but the emphasis is different. We think of F as coming first and L later.

Remark 4.2. If $F \subseteq L$ is a field extension, then L is in particular an F-vector space. This is a special case of the more general fact that if $\phi : R \to S$ is a ring homomorphism, then S is a left R-module via $r \cdot s := \phi(r)s$ by restriction of scalars.

Definition 4.3. The *degree* of a field extension L/F is

$$[L : F] = \dim_F(L).$$

A field extension is *finite* if its degree is finite.

Example. $[\mathbb{C} : \mathbb{R}] = 2, [\mathbb{Q}(\omega) : \mathbb{Q}] = 3$ and $[\mathbb{R} : \mathbb{Q}] = \infty$. We could in fact say $[\mathbb{R} : \mathbb{Q}]$ is the cardinality of $\mathbb{R}$, but in general we lump all infinite field extensions together when talking about degree.

Now we show that for any field and any non-constant polynomial, there exists a field extension in which the polynomial has at least one root.

Proposition 4.4. *If F is a field and $p(x) \in F[x]$ is irreducible and $L = F[x]/(p(x))$ then*

1. *L/F is a field extension via the map $F \to L, f \mapsto f + (p(x))$*
2. *$[L : F] = \deg(p)$*
3. *if $\bar{x} = x + (p(x)) \in L$ then $\bar{x}$ is a root of $p(x)$ in L*

Proof. Because $p(x)$ is irreducible, $(p(x))$ is a principal nonzero ideal and since all such ideals are maximal in a PID, we have that $F[x]/(p(x))$ is a field. We regard L as a field extension of F via the canonical map $F \to L$ sending $f \in F$ to the coset of the constant polynomial f.

The equality $[L : F] = \deg(p)$ holds since $1, x, \ldots, x^{n-1}$ is a basis for L regarded as an F-vector space (as shown on homework). Moreover, since $F \subseteq L$ we have $F[x] \subseteq L[x]$ and thus be can regard $p(x)$ as belonging to $L[x]$. Setting $\bar{x} = x + (p(x)) \in L$, we have that $\bar{x}$ is a root of $p(x) \in L[x]$ since $p(\bar{x}) = p(x) + (p(x)) = 0_L$.

□

Now that we know a field extension of F in which $p(x)$ has a root exists, we may wonder about the *smallest* such extension.

Definition 4.5. If $F \subseteq L$ is a field extension and $\alpha \in L$, we write $F(\alpha)$ for the smallest subfield of L that contains all of F and α. Since the intersection of any two subfields of L is again a subfield, $F(\alpha)$ exists and is

$$F(\alpha) = \bigcap_{E \text{ field }, F \cup \{\alpha\} \subseteq E \subseteq L} E.$$

Lemma 4.6. *If $F \subseteq L$ is a field extension and $\alpha \in L$, another way to describe this field $F(a)$ is as the fraction field of $F[\alpha] = \{f(\alpha) \mid f \in F[x]\}$, i.e.*

$$F(\alpha) = \left\{ \frac{g(\alpha)}{f(\alpha)} \mid g(x), f(x) \in F[x], f(\alpha) \neq 0 \right\}.$$

Proof. Exercise. □

We will give an even better description for $F(\sigma)$ in the case where α is the root of a polynomial $p \in F[x]$ below.

Definition 4.7. A field extension L/F is called *simple* if $L = F(\alpha)$ for some (typically, non-unique) element α of L. We call α a *primitive element* for the extension.

We can generalize this to adjoining a subset instead of a single element.

Definition 4.8. If $F \subseteq L$ is a field extension and A is any subset of L, we write $F(A)$ for the smallest subfield of L that contains all of F and A and it is called the subfield generated by A over F. Since the intersection of any two subfields of L is again a subfield, $F(A)$ exists and is

$$F(A) = \bigcap_{E, E \supseteq F \cup A} E.$$

Nearly always A will be a finite set, $A = \{a_1, \ldots, a_n\}$, and we write $F(a_1, \ldots, a_n)$ for $F(A)$.

Example. Regard $\mathbb{Q}$ as a subfield of $\mathbb{C}$ and let $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Note that we also have $F = E(\sqrt{3})$ where $E = \mathbb{Q}(\sqrt{2})$. We will see shortly that $E = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. In other words, E is the set of $\mathbb{Q}$-linear combinations of 1 and $\sqrt{2}$, so $[E : \mathbb{Q}] = 2$.

Likewise, we can see that F is the set of all E-linear combination of 1 and $\sqrt{3}$:

$$F = \{\alpha + \beta\sqrt{3} \mid \alpha, \beta \in E\} = \{(a + b\sqrt{2}) + (c + d\sqrt{2})\sqrt{3} \mid a, b, c, d \in \mathbb{Q}\}.$$

and we conclude that $[F : E] = 2$.

Next, I claim that F is in fact a simple extension of $\mathbb{Q}$. For example, say $\gamma = \sqrt{2} + \sqrt{3}$. I claim that $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = F$. Note that $\gamma^2 = 5 + 2\sqrt{6}$ and $\gamma^3 = 5\sqrt{2} + 5\sqrt{3} + 4\sqrt{3} + 6\sqrt{2} = 11\sqrt{2} + 9\sqrt{3}$. So $\frac{1}{2}(\gamma^3 - 9\gamma) = \sqrt{2}$, and hence $\sqrt{2} \in \mathbb{Q}(\gamma)$. Likewise, $\sqrt{3} = -\frac{1}{2}(\gamma^3 - 11\gamma) \in \mathbb{Q}(\gamma)$. So $\mathbb{Q}(\gamma) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

This example is an illustration of the Primitive Element Theorem (which we might or might not have time to prove this semester): Every finite extension of $\mathbb{Q}$ is generated by a single element, or is simple. This example shows $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ is simple and $\sqrt{2} + \sqrt{3}$ is a primitive element of this field extension.

March 11, 2019

Next we show that if α is a root of a given polynomial $p(x) \in F[x]$ then $F(\alpha)$ is determined by $p(x)$ up to isomorphism.

Theorem 4.9. *Let L/F be a field extension and let $p(x) \in F[x]$ be irreducible having a root $\alpha \in L$. Then there is an isomorphism $\phi : \frac{F[x]}{(p(x))} \to F(\alpha)$ given by $\bar{x} \mapsto \alpha$ so that $\phi|_F = \mathrm{id}_F$.*

Proof. Let $\tilde{\phi} : F[x] \to F(\alpha)$ be the evaluation homomorphism that sends $x \mapsto \alpha$ given by $\tilde{\phi}(f(x) = f(\alpha)$. Notice that the restriction of this map to F is the identity on F. Since $p(\alpha) = 0$, we have $(p(x)) \subseteq \mathrm{Ker}(\tilde{\phi})$ and since $(p(x))$ is a maximal ideal and $\mathrm{Ker}(\tilde{\phi}) \neq F[x]$, the equality $(p(x)) = \mathrm{Ker}(\tilde{\phi})$ must hold.

Now the UMP of the quotient ring yields an injective ring homomorphism

$$\phi : \frac{F[x]}{(p(x))} \hookrightarrow F(\alpha)$$

such that $\phi(f(x) + (p(x))) = \tilde{\phi}(f(x)) = f(\alpha)$.

It remains to be shown that ϕ is surjective. We will actually show more, namely that $\mathrm{Im}(\phi) = F[\alpha] = F(\alpha)$, where $F[\alpha] = \{f(\alpha) \mid f \in F[x]\}$. Note first that by the definition of ϕ above, the image of $\tilde{\phi}$ on $F[x]$ is $F[\alpha]$. However, since ϕ is injective the image of $\tilde{\phi}$ is a field contained in $F(\alpha)$ and since the smallest field containing $F[\alpha]$ is $F(\alpha)$ we must in fact have $\mathrm{Im}(\tilde{\phi}) = F(\alpha)$. □

Let's formalize the extra information we have obtained in the course of proving the theorem. First we used the following useful fact:

Remark 4.10. If $\phi : F \to L$ is an injective ring homomorphism and F, L are fields then the image of ϕ is a subfield of L.

Corollary 4.11. *Let L/F be a field extension and let $p(x) \in F[x]$ be irreducible having a root $\alpha \in L$. Then $F[\alpha] = F(\alpha)$.*

Corollary 4.12 (Uniqueness of $F(\alpha)$)**.** *Let $p(x) \in F[x]$ be irreducible and let α, α' be two roots of $p(x)$ in some extensions L, L' of F. Then $F(\alpha) \cong F(\alpha')$, i.e. the two roots are algebraically indistinguishable.*

Example. Taking $p(x) = x^2 + 1 \in \mathbb{R}[x]$ with roots $\alpha = i, \alpha' = -i$ in $\mathbb{C}$ we actually obtain *equal* fields $\mathbb{R}(i) = \mathbb{C} = \mathbb{R}(-i)$.

Example. Going back to the example $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\gamma)$ from before we want to find a polynomial $p \in \mathbb{Q}[x]$ such that $\mathbb{Q}(\gamma) \cong \mathbb{Q}[x]/(p(x))$.

Note that we have $\gamma^2 = 5 + 2\sqrt{6}$ and $\gamma^4 = 49 + 20\sqrt{6}$ and hence $\gamma^4 - 10\gamma^2 + 1 = 0$. So γ is a root of $x^4 - 10x^2 + 1$. It can be shown that this polynomial is irreducible, by reducing to showing that is irreducible in $\mathbb{Z}[x]$ which can be accomplished e.g. by reduction module 3. Hence setting $p(x) = x^4 - 10x^2 + 1$ gives the isomorphism above. This also shows that the degree of the extension is $[L : \mathbb{Q}] = 4$.

(We will see later that typically in a situation like this one first finds that $[L : F] = 4$ using the Degree Formula and then based on this knowledge that $[L : F] = 4 = \deg(x^4 - 10x^2 + 1)$ one can deduce $x^4 - 10x^2 + 1$ is irreducible by means of Theorem 4.14 below.)

March 13, 2019

4.1.2 Algebraic and transcendental extensions

Definition 4.13. For a field extension L/F and $\alpha \in L$, we say α is *algebraic over F* if $f(x) = 0$ for some non-constant polynomial $f(x)$. Otherwise, α is *transcendental over F*.

Example. $i \in \mathbb{C}$ is algebraic over $\mathbb{R}$. Indeed, every element of $\mathbb{C}$ is algebraic over $\mathbb{R}$. The numbers π and e of $\mathbb{R}$ are transcendental over $\mathbb{Q}$. These are deep facts.

Theorem 4.14. *Suppose L/F is a field extension and $\alpha \in L$.*

1. *The set $I := \{f(x) \in F[x] \mid f(\alpha) = 0\}$ is an ideal of $F[x]$.*
2. *$I = 0$ iff α is transcendental over F and $I \neq 0$ iff α is algebraic over F.*
3. *If α is algebraic over F (i.e., if $I \neq 0$), the unique monic generator of I, $m_{\alpha,F}(x)$, is irreducible.*
4. *If α is algebraic over F, then there is an isomorphism of fields*
$$F(\alpha) \cong F[x]/(m_{\alpha,F}(x))$$
sending F identically to F and sending x to α.
5. *α is algebraic over F if and only if $[F(\alpha) : F] < \infty$. In this case,*
$$[F(\alpha) : F] = \deg(m_{\alpha,F}(x)).$$
6. *α is transcendental over F if and only if $[F(\alpha) : F] = \infty$. In this case, there is an isomorphism of fields*
$$F(\alpha) \cong F(x)$$
sending F identically to F and sending x to α, where $F(x) = \{\frac{g(x)}{f(x)} \mid g \neq 0\}$ is the field of fractions of $F[x]$.

Proof. (1) follows because I is the kernel of the evaluation homomorphism that maps $x \mapsto \alpha$. (2) is by definition.

For (3), assume $I \neq 0$ and let $p(x)$ be its unique monic generator. Suppose $p(x) = f(x)g(x)$. Since $p(\alpha) = 0$ in F, either $f(\alpha) = 0$ or $g(\alpha) = 0$, giving that either $f(x) \in I$ or $g(x) \in I$. This proves $(p(x))$ is a prime ideal and hence p is prime. Since $F[x]$ is a PID, it follows that p is irreducible.

(4) is given by Theorem 4.9.

For (5), if α is algebraic over F, then (4) shows that $[F(\alpha) : F] = \deg(m_{\alpha,F}(x)) < \infty$. For the converse, if $[F(\alpha) : F] < \infty$, then the infinite list $1, \alpha, \alpha^2, \ldots$ of elements of $F(\alpha)$ cannot be F-linearly independent. So, $a_0 + a_1\alpha + \cdots a_n\alpha^n = 0$ for some n and some $a_0, \ldots, a_n \in F$ not all of which are 0. This shows α is the root of a non-zero polynomial.

For (6), the map ϕ defined as in (4) is injective. Since the target is a field L and $F[x]$ is an integral domain, by the UMP of the fraction field ϕ can be extended to the field of fractions of $F[x]$, i.e. there is a homomorphism of fields $\tilde{\phi} : F(x) \to L$. The image of this field map is $\left\{\frac{g(\alpha)}{f(\alpha)} \mid g, f \in \mathbb{F}[x], f(x) \neq 0\right\}$, which is precisely $F(\alpha)$ by Lemma 4.6 and the map is injective since it is a field homomorphism that is not identically zero. □

Definition 4.15. The unique monic generator of the ideal I in the previous theorem, denoted $m_{\alpha,F}(x)$, is called the *minimal polynomial of α over F*.

Remark 4.16. Note that the minimal polynomial of α over F (if it exists) divides every polynomial in $F[x]$ that has α as a root. Also, it can be characterized as the monic polynomial in $F[x]$ of least degree having α as a root. As a very simple example,

$$m_{i,\mathbb{R}}(x) = x^2 + 1.$$

Example. Going back to the example $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ from before where $\gamma = \sqrt{2} + \sqrt{3}$ and, we can argue that $m_{\gamma,\mathbb{Q}}(x) = x^4 - x^2 + 1$ as follows. By the degree formula 4.17 we have $[\mathbb{Q}(\gamma) : \mathbb{Q}] = [\mathbb{Q}(\gamma) : E][E : \mathbb{Q}] = 2 \cdot 2 = 4$ and so $m_{\gamma,\mathbb{Q}}(x)$ has degree 4. We already know that γ is a root of $x^4 - 10x^2 + 1$, hence this polynomial is divisible by the minimum polynomial of γ. Since they are both monic and have degree 4, it must be that $m_{\gamma,\mathbb{Q}}(x) = x^4 - 10x^2 + 1$. Arguing this way, there is no need to check this polynomial is irreducible; it must be by Theorem 4.14 (3).

Proposition 4.17 (The Degree Formula)**.** *Suppose $F \subseteq L \subseteq K$ are field extensions. Then*

$$[K : F] = [K : L][L : F].$$

In particular, the composition of two finite extensions of fields is again a finite extension.

March 15, 2019

Proof of the Degree Formula. Let $A \subseteq K$ be a basis for K as an L-vector space and let $B \subseteq L$ be a basis for L as an F-vector space. Let AB denote the subset $\{ab \mid a \in A, b \in B\}$ of K. The Proposition follows from the following two facts: (a) AB is a basis of K as an F-vector space and (b) the function $A \times B \to AB, (a, b) \mapsto ab$ is bijective (so that the cardinallity of AB is $|A| \cdot |B|$).

Concerning (a), for $\alpha \in K$, we have $\alpha = \sum_i l_i a_i$ for some $a_1, \ldots, a_m \in A$ and $l_1, \ldots, l_m \in L$. For each i, l_i is an F-linear combination of a finite set of elements of B. Combining these gives that α is in the F-span of AB.

To prove linear independence, it suffices to prove that if $a_1, \ldots, a_m$ and $b_1, \ldots, b_n$ be distinct elements of A and B respectively, then the set $\{a_i b_j\}$ is linearly independent. Suppose $\sum_{i,j} f_{i,j} a_i b_j = 0$ for some $f_{i,j} \in F$. Since the b_j's are L-linearly independent and $\sum_{i,j} f_{i,j} a_i b_j = \sum_j (\sum_i f_{i,j} a_i) b_j$ and $f_{i,j} a_i \in L$, we get that, for each j, $\sum_i f_{i,j} a_i = 0$. Using now that the a_i's are F-linearly independent, we have that for all j and all i, $f_{i,j} = 0$. This proves $\{a_i b_j \mid i = 1, \ldots, m, j = 1, \ldots, n\}$ is linearly independent over F, and hence AB is linearly indpendent over F.

Concerning (b), if $ab = a'b'$ for some $a, a' \in A, b, b' \in B$, then $ab - a'b' = 0$, and since the b's are L-linearly independent, we must have $b = b'$ and hence $a = a'$. □

Example. If w is an complex number that is not real, then $\mathbb{C} = \mathbb{R}(w)$. To see this, we use the degree formula

$$2 = [\mathbb{C} : \mathbb{R}] = [\mathbb{C} : \mathbb{R}(w)][\mathbb{R}(w) : \mathbb{R}].$$

Since $w \notin \mathbb{R}$, $\mathbb{R}(w)$ properly contains $\mathbb{R}$ and hence $[\mathbb{R}(w) : \mathbb{R}] \geq 2$. This forces $[\mathbb{R}(w) : \mathbb{R}] = 2$ and $[\mathbb{C} : \mathbb{R}(w)] = 1$, and the latter means $\mathbb{C} = \mathbb{R}(w)$.

Definition 4.18. A field extension L/F is called *algebraic* if every element $\alpha \in L$ is algebraic over F.

Remark 4.19. If L/F is a finite extension, then it is algebraic. This follows from the degree formula and part (5) of Theorem 4.14. The converse if false, as shown by the following example.

Example. $\overline{\mathbb{Q}}$, the set of complex numbers that are algebraic over $\mathbb{Q}$, is an algebraic extension of $\mathbb{Q}$. It is not finite over $\mathbb{Q}$, however because for every integer $n > 0$, $\overline{\mathbb{Q}}$ contains a sub-extensions of degree n of the form $\mathbb{Q}(\alpha)$ where α is the root of $x^n - p$, p any prime integer and the degrees of these subextensions are $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$.

It follows from the Degree Formula that if L/F and E/L are both finite field extensions, then E/F is algebraic. We prove something stronger next.

Proposition 4.20. *If L/F and E/L are both algebraic field extensions, then so is L/F.*

March 25, 2019

Proof. Pick $\alpha \in E$. We need to prove α is a root of some monic polynomial with coefficients in F. This is surprisingly hard to prove directly and indeed the proof is rather non-constructive.

Since α is algebraic over L, it is the root of some polynomial $a_n x^n + \cdots + a_1 x + a_0 \in L[x]$. Note that this polynomial belongs to $F(a_0, \ldots, a_n)[x]$ too, and so α is algebraic over $F(a_0, \ldots, a_n)$.

We consider the chain of field extensions

$$F \subseteq F(a_0) \subseteq F(a_0, a_1) \subseteq \cdots \subseteq F(a_0, a_1, \ldots, a_{n-1}) \subseteq F(a_0, \ldots, a_n, \alpha)$$

Since a_i is algebraic over F for all i and α is algebraic over $F(a_0, a_1, \ldots, a_n)$, by Theorem 4.14 each step in this chain has finite degree. By the Degree Formula, $[F(a_0, \ldots, a_n, \alpha) : F]$ is finite and thus so is $[F(\alpha) : F]$. By the Proposition again, α is algebraic over F. □

Remark 4.21. The converse of this proposition is also true: Given field extensions $F \subseteq L \subseteq K$, if K/F is algebraic then so are K/L and L/F. This is more or less obvious from the definition.

4.1.3 Algebraically closed fields and algebraic closure

Example. Let $\overline{\mathbb{Q}}$ be the collection of all complex numbers that are algebraic over $\mathbb{Q}$ — i.e., that are roots of polynomials with $\mathbb{Q}$-coefficients. For example, $i, \sqrt{5} \in \overline{\mathbb{Q}}$, but π does not belong to $\overline{\mathbb{Q}}$.

Proposition 4.20 (or really its proof) shows that $\overline{\mathbb{Q}}$ is a subfield of $\mathbb{C}$. For say $\alpha, \beta \in \overline{\mathbb{Q}}$. Then $\mathbb{Q}(\alpha)$ is finite over $\mathbb{Q}$ and $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha)(\beta)$ is finite over $Q(\alpha)$ since β is algebraic over $\mathbb{Q}$ and hence over $\mathbb{Q}(\alpha)$. It follows that $\mathbb{Q}(\alpha, \beta)$ is finite over $\mathbb{Q}$ and hence every element of $\mathbb{Q}(\alpha, \beta)$ belongs to $\overline{\mathbb{Q}}$. This includes each of $\alpha\beta$, α^{-1} (if $\alpha \neq 0$) and $\alpha + \beta$, which proves that $\overline{\mathbb{Q}}$ is a subfield of $\mathbb{C}$.

This example suggests the following definition:

Definition 4.22. For any field extension $F \subseteq L$, we define the *algebraic closure of F in L* to be the set $\overline{F}_L = \{\alpha \in L \mid \ \alpha \text{ is algebraic over } F\}$.

The argument of the previous example generalizes in a straightforward manner to prove:

Proposition 4.23. *For any field extension $F \subseteq L$, the set $\overline{F}_L$ is a a subfield of L that contains F. Moreover, it is the largest subfield of L that is algebraic over F.*

Proof. The last claim is obvious from the definition. It remains to show that $\overline{F}_L$ is a field, i.e. we need to show that $\overline{F}_L$ is closed under addition, multiplication and taking additive and multiplicative inverses. Say $\alpha, \beta \in \overline{F}_L$. Since α, β are algebraic over F and consequently β is algebraic over $F(\alpha)$ we have that $[F(\alpha) : F] < \infty$ and $[F(\alpha, \beta) : F(\alpha)] < \infty$. Thus by the degree formula the extension $F(\alpha, \beta)/F$ is finite hence algebraic. It follows that every element of $F(\alpha, \beta)$ is algebraic over F. In particular $\alpha \pm \beta, \alpha\beta, \alpha^{-1}$ are elements of $\overline{F}_L$. □

The notion of algebraic closure is closely related (pun intended) to being algebraically closed.

Definition 4.24. A field L is *algebraically closed* if every non-constant polynomial $f(x) \in L[x]$ has a root in L. This is equivalent to the condition that every non-constant polynomial splits completely into linear factors.

Example. $\mathbb{C}$ is algebraically closed. This follows from (actually is a restatement of) the Fundamental Theorem of Algebra, which says that any polynomial in $\mathbb{C}[x]$ has a root in $\mathbb{C}$.

Remark 4.25.

1. If L/F is a field extension with L algebraically closed, then $\overline{F}_L$ is also algebraically closed. This shows that the field $\overline{\mathbb{Q}}$ defined in example 4.1.3 is algebraically closed.

2. If L/F is a field extension with L not algebraically closed, then $\overline{F}_L$ need not be algebraically closed. For example, think of the extremal case when $F = L$. This forces that also $\overline{F}_L = F$.

Next we discuss the notion of algebraic closure.

Definition 4.26. Given a field F, a field $\overline{F}$ is called an *algebraic closure of* F if $\overline{F}$ is an algebraic field extension of F and $\overline{F}$ is algebraically closed.

Example.
- $\mathbb{C}$ is an algebraic closure of $\mathbb{R}$. This follows from the fact that $\mathbb{C}/\mathbb{R}$ is a finite extension, hence algebraic and the Fundamental Theorem of Algebra.
- $\overline{\mathbb{Q}}_{\mathbb{C}} = \{z \in \mathbb{C} \mid \ z \text{ is algebraic over } \mathbb{Q}\}$ is an algebraic closure of $\mathbb{Q}$. This is a consequence of the fact that an algebraic closure inside an algebraically closed field is algebraically closed by Remark 4.25 (1).

March 27, 2019

Theorem 4.27 (Existence and uniqueness of algebraic closures)**.** *For any field F, there exists an algebraic closure of F. If L and L' are two algebraic closures of the same field F, then there exists a field isomorphism $\phi : L \xrightarrow{\cong} L'$ such that $\phi|_F = id_F$.*

The proof is a bit long (and the uniqueness portion will be skipped in class). We start with:

Lemma 4.28. *If L/F is an algebraic field extension and every non-constant polynomial $f(x) \in F[x]$ splits completely into linear factors in $L[x]$, then L is algebraically closed and hence is an algebraic closure of F.*

Proof. Suppose $g(x) \in L[x]$ is not constant. We need to prove g has a root in L.

We may form a (possibly trivial) algebraic extension $L \subseteq E$ such that $g(x)$ has a root α in E. Note that E/F is algebraic and hence α is algebraic over F. So α is a root of some $f(x) \in F[x]$. But then $f(x) = \prod_i (x - \beta_i)$ in $L[x]$ and it follows that α must one of the β_i's and hence belongs to L. □

Proof of existence of algebraic closures. I will only sketch it.

I claim that there is an algebraic field extension $F \subseteq L$ such that every non-constant polynomial in $F[x]$ has at least one root in L. Grating this for the moment, by using this fact repeatedly, we may form a tower of field extensions

$$F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots$$

such that, for all i, $F_i \subseteq F_{i+1}$ is algebraic and every non-constant polynomial in $F_i[x]$ has at least one root in F_{i+1}. Let $E = \cup_i F_i$. It is not hard to show E is a field and it is clear that E is algebraic over F. Given $f(x) \in F[x]$, f has a root α in F_1 and hence factors as $f(x) = (x - \alpha)g(x)$ for $g(x) \in F_1[x]$. But then $g(x)$ has a root in F_2 and hence factors in $F_2[x]$. Repeating this we see $f(x)$ splits completely in $E[x]$. By the Lemma, E is an algebraic closure of F.

It remains to prove the claim. Let S be the collection of all non-constant polynomials with coefficients in F, and for each $f \in S$, pick an indeterminate y_f. Form the

rather large polynomial ring $R = F[\{y_f \mid f \in S\}]$. Let I be the ideal generated by $f(y_f)$. I claim that I is a proper ideal. Otherwise, we would have an equation of the form

$$1 = g_1 f_1(y_{f_1}) + \cdots g_m f_m(y_{f_m})$$

in R. We may find a finite extension E of F in which each f_i has a root α_i. Evaluating the above equation by setting $y_{f_i} = \alpha_i$ gives $1 = 0$, which is impossible.

Since I is proper, it is contained in some maximal ideal $\mathfrak{m}$ and for such an $\mathfrak{m}$, the quotient ring $K := R/\mathfrak{m}$ is a field. The composition $F \hookrightarrow R \twoheadrightarrow K$ is a ring map $F \to K$ between two fields, and is thus injective. We pretend it's an actual inclusion. For any $f \in S$, the image $\overline{y_f} \in K$ of $y_f \in R$ is a root of $f(x)$. That is, we have constructed a field exension $F \subseteq K$ such that every element f of S has a least one root in K. We are not quite done since it is not obvious that K is algebraic over F. For each $f \in S$, pick a root $\beta_f \in K$ of f. Let $L = F(\{\beta_f \mid f \in S\}) \subseteq K$. Then L is algebraic over F and every member of S has at least one root in L. □

Proof of uniqueness of algebraic closures. I only sketch it.

Suppose L and L' are two algebraic closures of F. Let $\mathcal{S}$ be the set of pairs (E, i) where E is a subfield of L that contains F and $i : E \hookrightarrow L'$ is a ring map with $i|_F = \mathrm{id}_F$. Make $\mathcal{S}$ into a poset by declaring that $(E, i) \leq (E', i')$ iff $E \subseteq E'$ and $i'|_E = i$.

It is relatively easy to see that $\mathcal{S}$ satisfies the hypotheses of Zorn's Lemma and hence has a maximal element (E, i). I claim E must equal L. If not, we can find $\alpha \in L \setminus E$. Let $p(x) = m_{\alpha,E}$ and set $E' := i(E)$. So i maps E isomorphically onto E'. Let $p'(x)$ be the polynomial in $E'[x]$ corresponding to $p(x)$ via i and pick any root α' of $p'(x)$ in L'. By Lemma **??**, there is an isomorphism $E(\alpha) \xrightarrow{\cong} E'(\alpha')$ extending the isomorphism i. Since $E'(\alpha) \subseteq L$ this contradicts the maximality of (E, i).

We have proven there is a ring map $i : L \hookrightarrow L'$ with $i|_F = \mathrm{id}_F$. In other words, we have field extensions $F \subseteq i(L) \subseteq L'$ with $i(L)$ isomorphic to L via an isomorphism fixing F. It follows that $i(L)$ is also an algebriac closure of F. Since L'/F is algebraic, we must have $i(L) = L'$. (In more detail, for $\beta \in L'$, we have $f(\beta) = 0$ for some $f(x) \in F[x]$. But since $i(L)$ is algebraically closed, all the roots of f must belong to $i(L)$.) □

4.1.4 Splitting fields

Definition 4.29. For a field F and non-constant polynomial $f(x) \in F[x]$, a *splitting field of $f(x)$ over F* is a field extension $F \subseteq L$ such that $f(x)$ splits completely into linear factors in $L[x]$, and f does not split completely into linear factors over any proper subfield of L that contains F.

Lemma 4.30. *If E/F is a field extension such that $f(x) \in F[x]$ splits into linear factors in $E[x]$ as $f(x) = c\prod_{i=1}^{n}(x - \alpha_i)$ for some $c, \alpha_i \in E$, then a splitting field for $f(x)$ over F is $F(a_1, \ldots, a_n)$. In other words, a splitting field is given by "adjoining all the roots" of a polynomial.*

Proof. Note that $f(x)$ also factors as $f(x) = \prod_{i=1}^{n}(x-\alpha_i)$ in $F(a_1, \ldots, a_n)[x]$ and hence, by the minimality condition in the definition, we must have $L \subseteq F(\alpha_1, \ldots, \alpha_n)$ for some splitting field L of $f(x)$ over F. However, the splitting field L must contain all roots of $f(x)$ in order for f to split completely in $L[x]$, i.e. we also have $F(\alpha_1, \ldots, \alpha_n) \subseteq L$. (Note that there may be repetitions in the list $\alpha_1, \ldots, \alpha_n$, but that does not affect the validity of anything here.) □

March 29, 2019

Example.
- As a silly example, if $f(x)$ already splits into linear factors over $F[x]$, then F itself is the splitting field of $f(x)$ over F.
- The splitting field of $x^2 + 1$ over $\mathbb{R}$ is $\mathbb{C}$.
- If $q(x)$ is any irreducible quadratic polynomial in $\mathbb{R}[x]$, then the splitting field of $q(x)$ is $\mathbb{C}$.
- The splitting field of $f(x) = (x^2 - 2)(x^2 - 3) = x^4 - 5x^2 + 6$ is

$$\mathbb{Q}(\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3}).$$

Remark 4.31. Note that in general if you want to form a field extension given by adjoining all the roots of two polynomial $g_1(x)$ and $g_2(x)$, then this amounts to forming a splitting field of their product $g_1(x)g_2(x)$.

Proposition 4.32. *For every field F and every non-constant polynomial $f(x)$ of degree $n \geq 1$, there exists a splitting field L for $f(x)$ over F with $[L : F] \leq n!$.*

Proof. Intuitively, we just need to adjoin all the roots of f, which is possible since we already know we can adjoint a root of any polynomial.

More formally, we start by showing that there is a field extension E/F such that $f(x)$ splits completely in $E[x]$ (but without the minimality condition). Proceed by induction on the degree of $f(x)$. If it is one, then f is linear and so $E = F$ works.

Assume f has degree more than one. We proved in Proposition 4.4 that there exists a field extension K of F such that $f(x)$ has a root α. (Recall how this goes: let $p(x)$ be any irreducibile factor of $f(x)$ and set $K = F[x]/(p(x))$ and $\alpha = x + (p(x))$.) So, in $K[x]$ we have $f(x) = (x - \alpha)g(x)$ with $\deg(g) < \deg(f)$. By induction, there is a field extension E of K with $[E : K] \leq (n-1)!$ in which $g(x)$ splits completely. Then f also splits completely in E and $[E : F] = [E : K][K : F] \leq (n-1)!n = n!$.

Finally, let $f(x) = \prod_i (x - \alpha_i)$ be the factorization of f in $E[x]$ and set $L = F(\alpha_1, \ldots, \alpha_n)$. By Lemma 4.30 L is a splitting field of f over F. □

I will give two examples of splitting fields, one that has degree $n!$ and one that has degree much smaller.

Example. Let's find the splitting field L of $x^3 - 2$ over $\mathbb{Q}$ and the degree of this field. It's roots (in $\mathbb{C}$) are $\sqrt[3]{2}$, $\zeta_3\sqrt[3]{2}$, and $\zeta_3^2\sqrt[3]{2}$, where $\zeta_3 = e^{\frac{2\pi i}{3}}$. So

$$L = \mathbb{Q}(\sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2}).$$

It is useful to simplify this a bit by noting that $\zeta_3 \in L$ (since it's the third element divided by the second) and that

$$L = \mathbb{Q}(\sqrt[3]{2}, \zeta_3).$$

We know from the Proposition above that $[L : \mathbb{Q}] \leq 6$. I claim it is exactly 6. We have

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq L$$

and $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ since $x^3 - 2$ is irreducible (Eisenstein) and hence must be the irreducible polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$. Note that $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$ but ζ_3 is not real. So $\mathbb{Q}(\sqrt[3]{2}) \subseteq L$ has degree at least two. The Degree Formula shows that $[L : \mathbb{Q}] = 6$.

Example. Let $f(x) = x^n - 1 \in \mathbb{Q}[x]$. Then $f(x)$ splits completely in $\mathbb{C}[x]$ and its roots are the n n-th roots of 1. One of these is $\zeta_n := e^{2\pi i/n}$. Notice that every other n-th root of 1 is a power of this one. We thus see that $\mathbb{Q}(\zeta_n)$ is the splitting field of $x^n - 1$ over $\mathbb{Q}$. This field is called the *cyclotomic field* of $n - th$ roots of 1 over $\mathbb{Q}$. This is a somewhat special example: upon joining one of the roots of f we got all the others for free. This happens in other examples too, but is certainly *not* a general principle.

Definition 4.33. Let $n \geq 2$ and let $\zeta_n = e^{2\pi i/n}$. The n-th *cyclotomic extension* is the extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$. The *primitive n-th roots of* 1 are the powers ζ_n^k for all $1 \leq k \leq n-1$ such that $\gcd(k, n) = 1$. The n-th *cyclotomic polynomial* is $\Phi_n = \prod_{1 \leq k \leq n-1, \gcd(k,n)=1}(x - \zeta_n^k)$. The *Euler totient function* is the function $\varphi : \mathbb{N} \to \mathbb{N}$ defined by $\varphi(n) := |\{k \mid 1 \leq k \leq n-1, \gcd(k, n) = 1\}|$.

April 1st, 2019

Proposition 4.34. *For all $n \geq 2$, the following are true*

1. $\Phi_n(x) \in \mathbb{Q}[x]$
2. $\Phi_n(x)$ *is irreducible in* $\mathbb{Q}[x]$, *thus* $m_{\zeta_n,\mathbb{Q}}(x) = \Phi_n(x)$
3. $\deg(\Phi_n(x)) = \varphi(n)$, *thus* $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$
4. $x^n - 1 = \prod_{d|n} \Phi_d(x)$

If $n = p$ is prime, then it can be shown that $x^{p-1} + \cdots + x + 1$ is irreducible by Eisenstein's Criterion (upon replacing x by $y + 1$). It follows that

$$m_{\zeta_p,\mathbb{Q}} = x^{p-1} + \cdots + x + 1.$$

In general, we can compute the n-th cyclotomic polynomial by factoring $x^n - 1$ into irreducible polynomials and picking the factor that has ζ_n as a root or we can use the formula $x^n - 1 = \prod_{d|n} \Phi_d(x)$ to compute the cyclotomic polynomials inductively. For example,

$$x^2 - 1 = (x+1)(x-1) \Longrightarrow m_{\zeta_2,\mathbb{Q}} = x + 1,$$

$$x^3 - 1 = (x+1)(x^2 - x + 1) \Longrightarrow m_{\zeta_3,\mathbb{Q}} = x^2 + x + 1,$$

$$x^4 - 1 = (x+1)(x-1)(x^2+1) \Longrightarrow m_{\zeta_4,\mathbb{Q}} = x^2 + 1,$$

$$x^6 - 1 = (x-1)(x+1)(x^2+x+1)(x^2-x+1) = \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x) \Longrightarrow m_{\zeta_6,\mathbb{Q}} = x^2+x+1,$$

Note that because the cyclotomic fields are subfields of $\overline{\mathbb{Q}}$ and the sequence of degrees of intermediate fields $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n) \to \infty$ as $n \to \infty$, we can conclude that $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$.

It seems intuitive that by adjoining all the roots of $f(x) \in F[x]$ to F, we will get a *unique* field (up to isomorphism). That is, it seems intuitive that splitting fields are unique up to isomorphism. This is indeed true, but the proof is a bit technical. We record here the result that gives the uniqueness of the splitting field noting that we postpone the technical details needed for the proof until the next section.

Corollary 4.35 (Uniqueness of the splitting field of $f(x)$ over the base field F)**.** *Any two splitting fields L, L' of $f(x) \in F[x]$ over F are isomorphic via an isomorphism $\phi : L \to L'$ that fixes F, i.e. $\phi|_F = id_F$.*

4.1.5 Separability

Definition 4.36. Let R be a commutative ring. The characteristic char(F) is defined to be the smallest positive integer n such that $n \cdot 1_F = \underbrace{1_F + \ldots + 1_F}_{n} = 0_F$, if such and integer exists, and 0 otherwise.

Example. $\mathrm{char}(\mathbb{Z}) = 0, \mathrm{char}(\mathbb{Z}/\mathrm{n}) = \mathrm{n}$.

Definition 4.37. For a field F its *prime field* is the subfield of F generated by 1_F.

Proposition 4.38. *Let F be a field.*

1. *The characteristic* char(F) *is either 0 or a prime number p.*
2. *The prime field of F is isomorphic to exactly one of the fields $\mathbb{Q}$ (iff* $\mathrm{char}(\mathrm{F}) = 0$*) or $\mathbb{Z}/p$ (iff* $\mathrm{char}(\mathrm{F}) = \mathrm{p}$ *for some prime number p).*

Proof. 1. Consider the ring homomorphism $\varphi : \mathbb{Z} \to F, \varphi(n) = n \cdot 1_F$. Since F is a domain, the kernel of φ is a prime ideal. Indeed, if $ab \in \mathrm{Ker}(\varphi)$ then $0 = \varphi(ab) = \varphi(a)\varphi(b)$ so $\varphi(a) = 0$ or $\varphi(b) = 0$, meaning that $a \in \mathrm{Ker}(\varphi)$ or $b \in \mathrm{Ker}(\varphi)$. Now since the prime ideals of $\mathbb{Z}$ are (0) and (p) for p any prime integer, the desired statement follows.

2. follows from 1. since the prime field is isomorphic to Frac(Im(φ)) and by 1.and the first isomorphism theorem we have that Im(φ) $\cong \mathbb{Z}$ or Im(φ) $\cong \mathbb{Z}/p$, hence Frac(Im(φ)) $\cong$ Frac($\mathbb{Z}$) $= \mathbb{Q}$ or Frac(Im(φ)) $\cong$ Frac($\mathbb{Z}/p$) $= \mathbb{Z}/p$. □

The most important tool we have at our disposal if char(R) = p, a prime, is the Frobenius endomorphism, also known as the Freshman's Dream.

Lemma 4.39 (Frobenius endomorphism = Freshman's Dream)**.** *If R is a commutative ring of prime characteristic p, then the following function is a ring homomorphism:*

$$\phi : R \to R, \quad \phi(c) = c^p$$

Proof. Since $(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{n-k}$ and the binomial coefficients $\binom{p}{k}$ are divisible by p for any $1 \leq k \leq p-1$, it follows that $(a+b)^p = a^p + b^p$. Because we also have $(ab)^p = a^p b^p$ by commutativity of R, the function ϕ is a ring homomorphism as desired. □

Remark 4.40. If R is a commutative ring of prime characteristic p, then, since End(R) is closed under composition, the n-th iterate of the Frobenius endomorphism

$$\phi^n = \underbrace{\phi \circ \cdots \circ \phi}_{n} : R \to R, \phi^n(x) = x^{p^n}$$

is also a ring homomorphisms.

Definition 4.41. For a field F and a polynomial $f(x) \in F[x]$ and a root α of $f(x)$ in some (any) field extension L of F, we define the *multiplicity of α in f* to be the number of times $x - \alpha$ appears in the factorization $f(x) = \prod_i (x - \alpha_i)$ of f in some (any) splitting field.

If the multiplicity of every root is 1, we say $f(x)$ is *separable*.

Example. $x^3 - 1$ is separable in $\mathbb{R}[x]$ because it has 3 distinct roots in $\mathbb{C}$, namely $1, \zeta_3, \zeta_3^2$, but not in $\mathbb{Z}/3[x]$ since $x^3 - [1]_3 = (x - [1]_3)^3$.

April 3, 2019

Definition 4.42. For any field F and $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in F[x]$, define its *derivative* to be

$$f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + 2a_2 x + a_1.$$

It is easy to see that the derivative is F-linear: For $f(x), g(x) \in F[x]$, $(f+g)' = f' + g'$ and $(af)' = af'$ for all $a \in F$.

Lemma 4.43 (Criteria for separability)**.** *1. Given $f(x) \in F[x]$ and a root α of f in some field extension L of F, the multiplicity of α in $f(x)$ is ≥ 2 if and only if $f'(\alpha) = 0$.*

2. *f is separable if and only if* $\gcd(f(x), f'(x)) = 1$ *in* $F[x]$.

3. *If $f(x)$ is irreducible in $F[x]$, then f is separable if and only if* $f'(x) \neq 0$.

Proof. Let L be the splitting field of $f(x)$. If $f(x) = (x-\alpha)^2 g(x)$ in $L[x]$, then $f'(x) = 2(x-\alpha)g(x) + (x-\alpha)^2 g(x)$. It follows that $f'(\alpha) = 0$. Conversely, if $f(x) = (x-\alpha)h(x)$ and $h(\alpha) \neq 0$, then $f'(x) = h(x) + (x-\alpha)h'(x)$ does not have α as a root.

The second assertion holds since $\gcd(f(x), f'(x)) = 1$ if and only if f and $f'(x)$ have no common roots in $\overline{F}$. (I leave it as an exercise; see below.)

For the final assertion, assume $f(x)$ is irreducible. Since the degree of $f'(x)$ is strictly less than the degree of $f(x)$, we have that $\gcd(f(x), f'(x)) \neq 1$ if and only if $f'(x) = 0$. □

Exercise 4.44. Prove that if F is a field and $f(x), g(x) \in F[x]$, then $\gcd(f, g) = 1$ if any only if f and g have no common roots in an algebraic closure $\overline{F}$ of F.

Definition 4.45. An algebraic field extension L/F is called *separable* if for every $\alpha \in L$ its minimum polynomial $m_{\alpha,F}(x)$ is separable.

Corollary 4.46. *If* $\mathrm{char}(F) = 0$*, then every irreducible polynomial in $F[x]$ is separable and every algebraic field extension L/F is separable.*

Proof. Since for every $\alpha \in L$ its minimum polynomial $m_{\alpha,F}(x)$ is non constant and $\mathrm{char}(F) = 0$ we have that $m'_{\alpha,F}(x) \neq 0$. Since $m_{\alpha,F}$ is irreducible in $F[x]$, Lemma 4.43 part 3. implies $m_{\alpha,F}(x)$ is separable. □

Proposition 4.47. *Let F be a field with* $\mathrm{char(F)} = \mathrm{p}$ *for some prime number p, and let K/F be an algebraic extension.*

1. *If b is an element of F that is not a p-th power of an element of F, and K/F is an algebraic extension of F that contains a root of $x^p - b$, then K/F is not separable.*

2. *If every element of F is the p-th power of another element of F, then every algebraic extension K/F is separable.*

Proof. 1. In general, for such an F and a, let α be a root of $x^p - b$ in some field extension of F and let $L = F(\alpha)$. I claim $F \subseteq L$ is not separable; specifically, I claim $p(x) := m_{\alpha,F}(x)$ is not separable. Since α is a root of $x^p - b$, we have $p(x) \mid x^p - b$. In $L[x]$, using the Freshman's Dream, we have

$$(x-\alpha)^p = x^p - \alpha^p = x^p - b.$$

If follows that $p(x)$ must divide $(x-\alpha)^p$ in $L[x]$ and hence must have the form $(x-\alpha)^i$ for some $1 \leq i \leq p$. But $i \neq 1$ since $\alpha \notin F$. Thus α is a multiple root of $p(x)$ and $p(x)$ is irreducible in $F[x]$.

2. Assume $\text{char}(F) = p$ and every element of F is the p-th power of another element. If $q'(x) = 0$, then we must have that $q(x)$ is a sum of terms of the form bx^{mp}, for $m \geq 0$, $b \in F$. By assumption, for each such term, we have $b = c^p$ for some $c \in F$, and thus each term of $q(x)$ has the form $(cx^m)^p$. By the Freshman's Dream, $q(x) = g(x)^p$ for some polynomial $g(x) \in F[x]$. But this is impossible since $q(x)$ is irreducible. □

April 5, 2019

Corollary 4.48. *Every algebraic field extension of a finite field is separable.*

Proof. Let F be a finite field. Then its prime subfield is also finite and hence isomorphic to $\mathbb{Z}/p$ for some prime integer p, thus char(F) = p. By the previous result, we just need to prove that the Frobenius endomorphism $\phi : F \to F$ defined by $\phi(c) = c^p$ is onto. But by the Freshman's Dream, ϕ is a ring homomorphism and, since F is a field, and $\phi \neq 0$, it is injective. Since $|F| < \infty$, ϕ must be onto by the pigeonhole principle. □

Fields which have the property that every one of their algebraic extensions is separable are called *perfect* fields. To summarize the section on separability, we have shown that fields of characteristic 0 and fields K of characteristic p such that $K = K^p$, in particular finite fields, are separable.

4.2 Galois theory

4.2.1 Group actions on field extensions

Definition 4.49. Let K be a field. The *automorphism group* of K, denoted $\text{Aut}(K)$, is the collection of field automorphisms of K, with the binary operation of composition.

Let K/F be a field extension. The *automorphism group* of K/F, denoted $\text{Aut}(K/F)$, is the collection of field automorphisms of K that restrict to the identity on F, with the binary operation of composition.

Lemma 4.50. *Let K/F be a field extension. Then* $\text{Aut}(K)$ *is a group and* $\text{Aut}(K/F)$ *is a subgroup of* $\text{Aut}(K)$.

Proof. Exercise. □

Example. $\text{Aut}(\mathbb{C}/\mathbb{R})$ has two elements, the identity and the element σ given as complex conjugation. It is easy to see each of these is an element of $\text{Aut}(\mathbb{C}/\mathbb{R})$. (For σ, this amounts to the fact that complex conjugation commutes with addition and multitplication of complex numbers.) To see these are all the automorphisms, suppose $\tau \in \text{Aut}(\mathbb{C}/\mathbb{R})$. For any $z = a + ib \in \mathbb{C}$, we have $\tau(z) = a + b\tau(i)$ since $\tau|_{\mathbb{R}} = \text{id}_{\mathbb{R}}$. Moreover, $-1 = \tau(-1) = \tau(i \cdot i) = \tau(i) \cdot \tau(i)$ and so $\tau(i) = \pm 1$.

Example. For any square-free integer d, $\mathrm{Aut}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$ also has two elements, the identity and the map sending $a + b\sqrt{d}$ to $a - b\sqrt{d}$. The details are similar to the previous example.

Definition 4.51. Let L be a field and let $\sigma \in \mathrm{Aut}(L)$. Then the UMP of polynomial rings gives that there is an induced ring homomorphism $(-)^\sigma : L[x] \to L[x]$ that maps $q(x) = a_n x^n + \cdots + a_0 \in K[x]$ let $q^\sigma(x) = \sigma(a_n)x^n + \cdots + \sigma(a_0)$. If $\sigma \in \mathrm{Aut}(L/K)$ and $q \in K[x]$, then $q^\sigma = q$.

Lemma 4.52. *Let K/F be a field extension, let $\sigma \in \mathrm{Aut}(K/F)$, and let $q \in F[x]$.*

1. *For all $k \in K, \sigma(q(k)) = q(\sigma(k))$.*
2. *If $b \in K$ is a root of q, then $\sigma(b)$ also is a root of q.*

Proof. 1. follows because σ is a homomorphism and it restricts to the identity on F.

2. If $\sigma \in \mathrm{Aut}(L/F)$ and $q(x) \in F[x]$, then we have $q^\sigma = q$. Since $\sigma(q(\alpha)) = q^\sigma(\sigma(\alpha))$ for all $\alpha \in L$, it follows that if α is a root of $f(x)$, then

$$0 = \sigma(q(\alpha)) = q^\sigma(\sigma(\alpha)) = q(\sigma(\alpha))$$

showing that $\sigma(\alpha)$ is also a root of $q(x)$. □

Next we give some technical results needed to prove some nice properties of $\mathrm{Aut}(L/F)$ for the case of splitting fields L.

Lemma 4.53. *Given a field F, a non constant polynomial $f(x)$, and a field isomorphism $\theta : F \to F'$, let $g = \tilde{\theta}(f) \in F'[x]$ be the polynomial corresponding to f under the induced isomorphism $\tilde{\theta} : F[x] \to F'[x]$.*

1. *If f is irreducible and α is any root of $f(x)$ in some field extension L of F and α' is any root of $g(x)$ in some field extension L' of F'. Then there exists a field isomorphism*
$$\widehat{\theta} : F(\alpha) \xrightarrow{\cong} F'(\alpha')$$
that extends the map θ and sends α to α'.
2. *Suppose L is a splitting field of f over F and L' is a slitting field of g over F'. Then there is a field isomorphism $\widehat{\theta} : L \to L'$ extending θ.*

Proof. 1. The key point is that

$$F[x]/(f(x)) \cong F(\alpha)$$

via a map that is the identity on F and sends x to α, as we saw before. Thus we have

$$F(\alpha) \cong F[x]/(f(x)) \cong F'[x]/(g(x)) \cong F'(\alpha')$$

with the middle isomorphism induced by θ. Tracking through these maps reveals that it extends θ and sends α to α'.

2. We proceed by induction on the degree of f. If f is linear then so is f' and in this case $L = F$ and $L' = F'$, so that there is nothing to prove.

Let $p(x)$ be any irreducible factor of f, let $\alpha \in L$ be any one of the roots of p. Let $q(x) = \tilde{\theta}(p)$ be the irreducible polynomial in $F'[x]$ that corresponds to $p(x)$, and let α' be any one of the roots of q. By part 1, there is an isomorphism $\phi : F(\alpha) \xrightarrow{\cong} F'(\alpha')$ extending θ and sending α to α'.

In $F(\alpha)$, $f(x)$ factors as $(x-\alpha)h(x)$, and in $F'(\alpha')$, $g(x) = (x-\alpha')\ell(x)$. Moreover, since ϕ extends θ and $\phi(\alpha) = \alpha'$, it follows that ϕ sends $f(x)$ to $g(x)$ and that it sends $x - \alpha$ to $x - \alpha'$. It thus must also send $h(x)$ to $\ell(x)$.

Note that L is a splitting field of h over $F(\alpha)$ and L' is a splitting field of ℓ over $F(\alpha')$. Since $\deg(h) < \deg(f)$, it follows by induction that there is a field isomorphism $\widehat{\theta} : L \to L'$ that extends ϕ and hence extends θ. □

April 8, 2019

Lemma 4.53 gives as a particular case the statement announced before regarding the uniqueness of the splitting field of a polynomial.

Corollary 4.54 (Uniqueness of the splitting field)**.** *Given a field F, a non constant polynomial $f(x)$, and two splitting fields L and L' for f over F, there is a field isomorphism $\hat{\theta} : l \to L'$ such that $\hat{\theta}|_F = id_F$.*

Proof. Apply part (2) of Lemma 4.53 to $\theta = \mathrm{id}_F$. □

We now come to the main idea connecting filed extensions and groups. It concerns the action of the group of automorphisms of a splitting field of a polynomial on the set of roots of that polynomial.

Consult Definition 1.32 for a reminder of the definition of a group action, Definition 1.100 for the definition of a faithful group action and Definition 1.101 for the definition of a transitive group action.

Theorem 4.55. *Let K/F be the splitting field of a polynomial $q \in F[x]$. Let S be the set of distinct roots of q in K, and let $n = |S|$.*

1. *$Aut(K/F)$ acts faithfully on Y, via $\sigma \cdot b = \sigma(b)$ for all $\sigma \in \mathrm{Aut}(K/F)$ and $b \in Y$, and hence $\mathrm{Aut}(K/F)$ is isomorphic to a subgroup of S_n.*

2. *If f is an irreducible polynomial in $F[x]$, then $\mathrm{Aut}(K/F)$ acts transitively on S.*

3. *The orbits of the action of $\mathrm{Aut}(K/F)$ on S are the subsets of S that are the roots of the same irreducible factor of q.*

Proof. 1. Let $G = Aut(K/F)$. To see that the the action claimed above is well defined notice that if $b \in S$ then $\sigma(b) \in S$ by Lemma 4.52. Now we have

$$\sigma \cdot \sigma' \cdot b = \sigma(\sigma'(b)) = (\sigma \circ \sigma')(b), \quad \forall \sigma, \sigma' \in G, b \in S$$

$$1_G \cdot b = \mathrm{id}_K(b) = b, \quad \forall \sigma \in G, b \in S$$

so the given formula indeed defines an action of G on S.

The action is faithful since if σ fixes all the roots $\alpha_1, \ldots, \alpha_n$ of f, then it fixes every element of $F(\alpha_1, \ldots, \alpha_n) = L$.

2. Now assume $f(x)$ is an irreducible polynomial. Let α, β be any two roots of $f(x)$. Lemma 4.53(1) shows there is an isomorphism $\theta : F(\alpha) \to F(\beta)$ that fixes F.

We have $f(x) = (x - \alpha)g(x)$ and $f(x) = (x - \beta)h(x)$.Since $f^\theta = f$ and $(x - \alpha)^\theta = x - \beta$, we must have $g^\theta(x) = h(x)$. Lemma 4.53(2) applies to show there is an automorphism $\sigma : L \to L$ that extends θ. It is clear that σ fixes F (i.e., $\sigma \in \mathrm{Aut}(L/F)$) and satisfies $\sigma(\alpha) = \beta$. This proves the action is transitive on the set of roots of any irreducible polynomial.

3. For each $b \in S$ the orbit of b is $\{\sigma(b) \mid \sigma \in \mathrm{Aut}(K/F)\}$. Since b is a root of $f(x)$ there exists an irreducible factor $p(x) \in F[x]$ of $f(x)$ such that b is a root of $p(x)$. Then, since $p(x) \in F[x]$, Lemma 4.52 shows that $\sigma(b)$ will be a root of $p(x)$ for any $\sigma \in \mathrm{Aut}(K/F)$. Thus the orbit of b is contained in the set of roots of $p(x)$ in K.

Conversely, since by part (2) $\mathrm{Aut}(K/F)$ acts transitively on the set of roots of $p(x)$, we have that every root of $p(x)$ is in the orbit of b under the action of $\mathrm{Aut}(K/F)$, hence the desired conclusion follows. □

From part (1) of the theorem we deduce the following

Corollary 4.56. *Let K/F be the splitting field of a polynomial $q \in F[x]$ having n distinct roots. Then $|\mathrm{Aut}(K/F)| \leq n!$.*

We shall give an improved version of this result shortly.

April 10, 2019

A typical question that arises from Theorem 4.55 is to identify the automorphisms of a splitting field extension as a subgroup of the symmetric group.

Example. Let's compute $G := \mathrm{Aut}(L/\mathbb{Q})$ where L is the splitting field of $x^3 - 2$. Recall that $L = \mathbb{Q}(\sqrt[3]{2}, \zeta)$ where $\zeta = e^{2\pi i/3}$ and that $[L : \mathbb{Q}] = 6$. Let us write the roots of $x^3 - 2$ as $\alpha_1 = \sqrt[3]{2}, \alpha_2 = \zeta\alpha_1, \alpha_3 = \zeta^2\alpha_1$. From Theorem 4.55, G acts transitively on $\{\alpha_1, \alpha_2, \alpha_3\}$ and hence is isomorphic to a subgroup of S_3.

The restriction of complex conjugation to L determines an element σ of G or order 2 since L is closed under complex conjugation. On the roots we have $\sigma(\alpha_1) = \alpha_1, \sigma(\alpha_2) = \alpha_3, \sigma(\alpha_3) = \alpha_2$ and so σ corresponds to $(2\,3) \in S_3$.

Since the action of G on the roots of $x^3 - 2$ is transitive, there is also an element $\tau \in G$ such that $\tau(\alpha_1) = \alpha_2$. Such a τ corresponds to either $(1\,2)$ or $(1\,2\,3)$ of S_3. Either way, τ and σ generated all of S_3.

We conclude that $|G| = 6$, the maximum possible, and G is isomorphic to S_3. You should think of this as saying that the roots of $x^3 - 2$ are as interchangeable as possible, since $\mathrm{Aut}(L/\mathbb{Q})$ is as large as possible.

Example. Let L be the splitting field of $x^4 - 2$ over $\mathbb{Q}$. The roots are $\alpha_1 = \sqrt[4]{2}$, $\alpha_2 = i\alpha_1$, $\alpha_3 = -\alpha_1$, $\alpha_4 = -i\alpha_1$. We have $L = \mathbb{Q}(\alpha_1, i)$. Let's start by computing $[L : \mathbb{Q}]$. For this the chain of extensions

$$\mathbb{Q} \subset \mathbb{Q}(\alpha_1) \subset L = \mathbb{Q}(\alpha_1)(i)$$

is useful. The first has degree 4, since $x^4 - 2$ is irreducible by Eisenstein, and the second has degree at most 2. Since $\mathbb{Q}(\alpha_1) \subset \mathbb{R}$ and L is not, the second extension cannot be trivial and so must have degree exactly 2. We conclude $[L : \mathbb{Q}] = 8$.

Set $G = \mathrm{Aut}(L/\mathbb{Q})$. We know G is isomorphic to a subgroup of S_4. Since $L = \mathbb{Q}(\alpha_1, i)$, any $\tau \in G$, is uniquely specified by what it does to α_1 and i (see problem 1 on Hw 12). Such a τ must send α_1 to one of $\alpha_1, \ldots, \alpha_4$ and i to $\pm i$ (since i is a root of $x^2 + 1$ which has rational coefficients). This gives at most 8 possibilities and so $\#G \leq 8$. In particular, G corresponds to a *proper* subgroup of S_4, and so the roots of $x^4 - 2$ do not have as many symmetries as are conceivabale.

Claim: $|G| = 8$ and G is isomorphic to the subgroup of S_4 generated by $(2\,4)$ and $(1\,2\,3\,4)$. (This is isomorphic to D_8.)

Let $\sigma \in \mathrm{Aut}(L/\mathbb{Q})$ be complex conjugation restricted to L. Then σ corresponds to $(2\,4) \in S_4$.

To construct the other element, we consider the field extension $L/\mathbb{Q}(i)$. Since $[L : \mathbb{Q}] = 8$ and $[\mathbb{Q}(i) : \mathbb{Q}] = 2$, we must have $[L : \mathbb{Q}(i)] = 4$. Since $L = \mathbb{Q}(i)(\alpha_1)$, the degree of $m_{\alpha_1, \mathbb{Q}(i)}$ must be 4. This shows that $x^4 - 2$ remains irreducible as a polynomial in $\mathbb{Q}(i)[x]$. (This is not obvious, but we have now proven it.) So L is the splitting field of the irreducible polynomial $x^4 - 2$ over $\mathbb{Q}(i)$, and we may thus apply Theorem 4.55(2) to get that there is an element $\tau \in \mathrm{Aut}(L/\mathbb{Q}(i))$ such that $\tau(\alpha_1) = \alpha_2$. We may regard τ as an element of $\mathrm{Aut}(L/\mathbb{Q})$ too. We have

$$\tau(\alpha_2) = \tau(i\alpha_1) = i\tau(\alpha_1) = ii\alpha_2 = \alpha_3$$

since $\tau(i) = i$ by construction. A key point here is that if we had merely specificed τ to be an element of $\mathrm{Aut}(L/\mathbb{Q})$ sending α_1 to α_2, then we would have no idea what τ does to α_2 — it was key to define $\tau \in \mathrm{Aut}(L/\mathbb{Q}(i))$ as we did. We then also get $\tau(\alpha_3) = \alpha_4$ and $\tau(\alpha_4) = \alpha_1$. So τ corresponds to the permutation $(1\,2\,3\,4)$.

The proves that G is isomorphic to a subgroup of S_4 that contains $(2\,4)$ and $(1\,2\,3\,4)$. Since the subgroups generated by these two elements has order 8 and $|G| \leq 8$, we must have equality as claimed.

4.2.2 Galois extensions and the FTGT

Theorem 4.57. *Let L/F be a finite field extension. Then:*

1. $|\operatorname{Aut}(L/F)| \leq [L : F]$

2. *If L is the splitting field of a separable polynomial in $F[x]$, then*

$$|\operatorname{Aut}(L/F)| = [L : F].$$

Definition 4.58. A *finite* field extension L/F is *Galois* if $|\operatorname{Aut}(L/F)| = [L : F]$. In this case we write $\operatorname{Gal}(L/F)$ instead of $\operatorname{Aut}(L/F)$, and $\operatorname{Gal}(L/F)$ is the *Galois group of L over F*.

Corollary 4.59 (First construction of Galois extensions from splitting fields)**.** *If L is the splitting field of a separable polynomial $f(x) \in F[x]$, then L/F is Galois.*

April 12, 2019

Proof of Theorem 4.57.

1. To prove the first assertion, we proceed by induction on $[L : F]$.

The base case, $[L : F] = 1$ is obvious.

Pick $\alpha \in L \setminus F$ and let $p(x) = m_{\alpha,F}(x)$. Consider $F(\alpha)/F$.

Note that $H = \operatorname{Aut}(L/F(\alpha))$ is a subgroup of $G = \operatorname{Aut}(L/F)$, and that by induction we have $|H| \leq [L : F(\alpha)]$. Using the degree formula and the fact that $|G| = |H| \cdot [G : H]$, it suffices to prove $[G : H] \leq [F(\alpha) : F]$.

Claim: the function

$$G/H = \{\text{cosets of } H \text{ in } G\} \to \{\text{roots of } p(x) \text{ in } L\} \tag{4.2.1}$$

given by $gH \mapsto g(\alpha)$ is well-defined and injective.

Recall that for any $g \in G$, we have that $g(\alpha)$ is also a root of $p(x)$, and since for any $h \in H$ $gh(\alpha) = g(h(\alpha)) = g(\alpha)$ this function is well defined. For $g_1, g_2 \in G$, we have $g_1(\alpha) = g_2(\alpha)$ iff $g_2^{-1} g_1(\alpha) = \alpha$ iff $g_2^{-1} g_1 \in H$. This proves that the function is injective. Since $\deg(p(x)) = [F(\alpha) : F]$, we conclude from the claim that $[G : H] = |G/H| \leq [F(\alpha) : F]$.

2. Now assume L is splitting field of a separable polynomial $f(x)$, so that $f = c \prod_{i=1}^{n} (x - \alpha_i)$ with $\alpha_i \neq \alpha_j$ for $i \neq j$ and $L = F(\alpha_1, \ldots, \alpha_n)$. We also proceed by induction on $[L : F]$.

Set $\alpha = \alpha_1$ and let $p(x)$ denote the irreducible factor of $f(x)$ that has α as a root. As before we consider $F(\alpha)$ and set $H = \operatorname{Aut}(L/F(\alpha)) \leq \operatorname{Aut}(L/F) = G$. Note that L is splitting field of $g(x) = \prod_{i=2}^{n} (x - \alpha_i) \in F(\alpha)[x]$ over $F(\alpha)$, and $g(x)$ is also separable. So, by induction $|H| = [L : F(\alpha)]$ and it remains to prove $[G : H] = [F(\alpha) : F] = \deg(p)$. Since f is separable, so is p, so $\deg(p)$ is the number of distinct roots of p. Then showing that $[G : H] = \deg(p)$ amounts to the assertion that the injective map (4.2.1) is also surjective. But this holds since G acts transitively on the roots of $p(x)$ by Theorem 4.55(2). □

Example (A non-example)**.** The field extension $L = \mathbb{Q}(\sqrt[3]{2})$ of $\mathbb{Q}$ is not Galois. Indeed, suppose $\sigma \in \mathrm{Aut}(L/\mathbb{Q})$. Then σ is entirely determined by where it sends $\sqrt[3]{2}$ and it must send this element to another root of $x^3 - 2$. But the other two roots of this polynomial are not real and hence not in L. So $\sigma = \mathrm{id}$.

This shows $\mathrm{Aut}(L/\mathbb{Q})$ is the trivial group of order 1 which is less that $[L : \mathbb{Q}] = 3$.

Definition 4.60. If $f(x) \in F[x]$ is a separable polynomial, the *Galois group of* $f(x)$ is $\mathrm{Gal}(L/F)$ where L is the splitting field of $f(x)$ over F.

We now proceed to a second construction for Galois extensions.

Definition 4.61. If G is subgroup of $\mathrm{Aut}(L)$, the *subfield of* L *fixed by* G, denoted L^G, is by definition $L^G := \{\alpha \in L \mid \sigma(\alpha) = \alpha, \text{ for all } \sigma \in G\}$. (Our text writes this as L_G.)

The following is an important theorem with many corollaries. In fact, the Fundamental Theorem of Galois Theory, which we will state shortly, is arguably a Corollary of this result.

Theorem 4.62 (Second construction of Galois extensions = Artin's Theorem)**.** *Let* L *be any field and* G *any finite subgroup of* $\mathrm{Aut}(L)$*. Then* L^G *is a subfield of* L*,* L/L^G *is a finite Galois extension and* $\mathrm{Gal}(L/L^G) = G$*.*

Note that I really do mean equality here: both G and $\mathrm{Gal}(L/L^G)$ are subgroups of $\mathrm{Aut}(L)$, and the theorem states that they coincide. The containment $G \subseteq \mathrm{Gal}(L/L^G)$ is clear: If $\sigma \in G$, then by construction σ fixes every element of L^G and hence $\sigma \in \mathrm{Gal}(L/L^G)$. So the point of the theorem is that $L^G \subseteq L$ really is Galois and that if $\sigma \in \mathrm{Aut}(L)$ fixes every element of L^G then σ must belong to G.

I will not prove Artin's Theorem right away. Instead, I'll deduce some consequences of it, including the Fundamental Theorem of Galois Theory. I will then illustrate the Fundamental Theorem with many examples and give some consequences of it too. Finally, we'll circle back to prove Artin's Theorem.

Example. The group $G = \{\mathrm{id}_{\mathbb{C}}, \sigma\}$ where σ is complex conjugation, is a finite subgroup of $\mathrm{Aut}(\mathbb{C})$. Artin's Theorem tells us that $\mathbb{C}^G \subseteq \mathbb{C}$ is finite and Galois with Galois group G. It follows that $[\mathbb{C} : \mathbb{C}^G] = |G| = 2$. Of course, this is all correct since we know $\mathbb{R} = \mathbb{C}^G$.

As we head towards the Fundamental Theorem of Galois Theory, we start by stating a few helpful corollaries of Artin's Theorem. These will also allow us to show that finite Galois extensions are precisely the splitting fields of separable polynomials.

Corollary 4.63 (Equivalence of the two constructions)**.** *A finite field extension* L/F *is Galois if and only if it is the splitting field of some separable polynomial* $f(x) \in F[x]$ *with coefficients in* F*.*

Definition 4.64. Given a field extension $F \subseteq L$, an *intermediate field* is a subfield E of L that contains F, so that $F \subseteq E \subseteq L$.

Corollary 4.65. *If L/F is a (finite) Galois extension, then so is L/E for any intermediate field E.*

Proof. This is immediate from the previous Corollary. Indeed, if L is the splitting field over F of a separable polynomial $f(x) \in F[x]$, then L is also the splitting field over E of the same polynomial. □

April 15, 2019

Remark 4.66 (**Warning!**). In the setting of the previous Corollary, E need not be Galois over F. For example, $L = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$ is Galois over $F = \mathbb{Q}$ but $E = \mathbb{Q}(\sqrt[3]{2})$ is not Galois over $\mathbb{Q}$.

We now arrive at the FTGT:

Theorem 4.67 (Fundamental Theorem of Galois Theory)**.** *Suppose L/F is a finite Galois extension. Then the function*

$$\Psi : \{\textit{intermediate fields } E, \textit{ with } F \subseteq E \subseteq L\} \to \{\textit{subgroups } H \textit{ of } \mathrm{Gal}(L/F)\}$$

$$\Psi(E) = \mathrm{Gal}(L/E)$$

is a bijection with inverse $\Psi^{-1}(H) = L^H$ for any $H \leq \mathrm{Gal}(L/F)$. Moreover, this correspondence enjoys the following properties:

1. *Ψ and Ψ^{-1} each reverse the order of inclusion.*
2. *Ψ and Ψ^{-1} convert between degrees of extensions and indices of subgroups:*
   - $[\mathrm{Gal}(L/F) : H] = [L^H : F]$ *or, equivalently,*
   - $[\mathrm{Gal}(L/F) : \mathrm{Gal}(L/E)] = [E : F]$.
3. *Normal subgroups correspond to intermediate fields that are Galois over F:*
   - *If $N \trianglelefteq G$ then L^N/F is Galois.*
   - *If E/F is Galois, then* $\mathrm{Gal}(L/E)$
4. *If $E = L^N$ for a normal subgroup $N \trianglelefteq \mathrm{Gal}(L/F)$, then* $\mathrm{Gal}(E/F) \cong \mathrm{Gal}(L/F)/N$.
5. *If H_1, H_2 are subgroups of G with fixed subfields $E_1 = L^{H_1}$ and $E_2 = L^{H_2}$, then*
   (a) *$E_1 \cap E_2 = L^{<H_1, H_2>}$ and* $\mathrm{Gal}(L/E_1 \cap E_2) = \langle H_1, H_2 \rangle$
   (b) *$E_1E_2 = L^{H_1 \cap H_2}$ and* $\mathrm{Gal}(L/E_1E_2) = H_1 \cap H_2$.

Corollary 4.68. *The Gallois correspondence induces a lattice isomorphism between the lattice of intermediate fields of a Galois extension L/F and the dual of the lattice of subgroups of* $\mathrm{Gal}(L/F)$.

Example. Let L be the splitting field of $x^4 - 2$ over $\mathbb{Q}$. Let's use the fundamental theorem to list all intermediate fields for $L/\mathbb{Q}$ and to determine which are Galois over $\mathbb{Q}$.

We know $G := \mathrm{Gal}(L/\mathbb{Q})$ corresponds to the 8 element subgroup of S_4 generated by $\sigma = (2\,4)$ and $\tau = (1\,2\,3\,4)$ where we number the roots as $\alpha_1 = \sqrt[4]{2}, \alpha_2 = i\alpha_1, \alpha_3 = -\alpha_1, \alpha_4 = -i\alpha_1$.

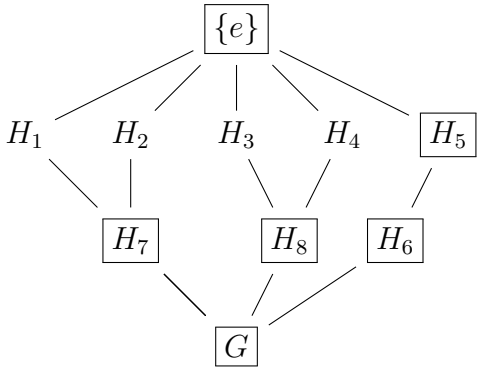
This group is isomorphic to D_8 and we can make this isomorphism explicit by labeling the four corners of a square by $\alpha_1, \ldots, \alpha_4$, counter-clockewise. So, τ is rotation by 90 degrees and σ is reflection about the line joining vertices 1 and 3.

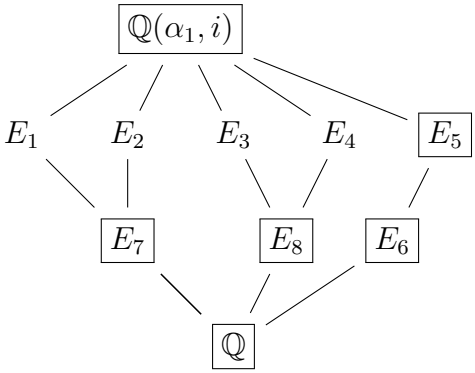
The subgroup lattice and intermediate field lattice are represented below, with normal subgroups and Galois extensions highlighted (boxed).

The subgroups are

$$\begin{aligned} G &= \langle (2\,4), (1\,2\,3\,4) \rangle \\ \{e\} & \\ H_1 &= \langle (2\,4) \rangle \\ H_2 &= \langle (1\,3) \rangle \\ H_3 &= \langle (1\,2)(3\,4) \rangle \\ H_4 &= \langle (1\,4)(2\,3) \rangle \\ H_5 &= \langle (1\,3)(2\,4) \rangle \\ H_6 &= \langle (1\,2\,3\,4) \rangle \\ H_7 &= \langle (1\,3), (2\,4) \rangle \\ H_8 &= \langle (1\,2)(3\,4), (1\,4)(2\,3) \rangle \end{aligned}$$

and the lattices are





The intermediate fields are the fixed subfields of L associated to each of these subgroups. In some sense, this answers the quesiton, but let's find explicit generators for at least some of these.

G corresponds to $\mathbb{Q}$ and e corresponds to $L = \mathbb{Q}(\alpha_1, i)$.

Set $E_i = L^{H_i}$.

E_1 has degree $4 = [G : H_1]$ over $\mathbb{Q}$. It is clear α_1 (and α_3) belongs to E_1 and since $[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = 4$, we must have $E_1 = \mathbb{Q}(\alpha_1)$.

Likewise $E_2 = \mathbb{Q}(\alpha_2)$.

E_3 also has degree four over $\mathbb{Q}$. Let $\beta = \alpha_1 + \alpha_2 = (1+i)\sqrt[4]{2}$ and note $\beta \in E_3$. If $[\mathbb{Q}(\beta) : \mathbb{Q}] = 2$, then β would be fixed by a subgroup of index 2 that contains $(1\,2)(3\,4)$, and the only possibility is H_8. But $(1\,4)(2\,3)$ sends β to $\alpha_4 + \alpha_3 = -\beta \neq \beta$. So we must have $[\mathbb{Q}(\beta) : \mathbb{Q}] = 4$ and hence $E_3 = \mathbb{Q}(\beta)$.

I'll skip the details on E_4 and E_5, but they are $E_4 = \mathbb{Q}((1-i)\alpha_1)$ and $E_5 = \mathbb{Q}(\sqrt{2}, i)$.

E_6 has degree equal to $[G : H_6] = 2$ over $\mathbb{Q}$ and so we merely need to find a single, non-rational element of L fixed by τ. Since $\tau(i) = i$ (which can be seen by looking back at how we built τ originally or by noting that $\tau(i) = \tau(\alpha_2/\alpha_1) = \alpha_3/\alpha_2 = i$), we get $E_6 = \mathbb{Q}(i)$.

I'll skip the details on E_7, but it is $E_7 = \mathbb{Q}(\sqrt{2})$.

E_8 also has degree two over $\mathbb{Q}$ and so we just need to find a single non-rational element fixed by the two generators of H_8. Note that $\alpha_1\alpha_2 = \alpha_3\alpha_4 = i\sqrt{2}$ and so $i\sqrt{2}$ is fixed by both $(1\,2)(3\,4)$ and $(1\,4)(2\,3)$. Thus $E_8 = \mathbb{Q}(i\sqrt{2})$.

Finally, we note that $G, \{e\}, H_5, H_6, H_7, H_8$ are normal subgroups of D_8, since H_5 is the center of D_8 and each of H_6, H_7, H_8 has index two. Some messy checking reveals these to be the only normal subgroups. It follows from the Fundamental Theorem that $\mathbb{Q}, L, E_5, E_6, E_7, E_8$ are the only intermediate fileds that are Galois over $\mathbb{Q}$. As an example, to see directly that E_3 is not Galois over $\mathbb{Q}$, note that $(1+i)\sqrt[4]{2}$ is a root of $x^4 + 4$, which is irreducible. But $(1-i)\sqrt[4]{2}$ is also a root of this polynomial and it is not in E_3.

April 17, 2019

4.2.3 Proof of Artin's Theorem and the FTGT

We now embark on a proof of Artin's Theorem. A key ingredient is the "linear independence of characters", which is useful in other contexts as well, such as representation theory (a 901 topic).

Definition 4.69. For a group G and field F, a *character* (of G with values in F) is a group homomorphism of the form

$$\chi : G \to F^\times$$

where, recall, $F^\times$ denotes the set of non-zero field elements viewed as a group under multiplication.

Example.

- If $G = C_n$, cyclic of order n, with generator x, then the UMP for cyclic groups says there is a unique group homomorphism $G \to \mathbb{C}^\times$ sending $x \mapsto \zeta_n$ (and hence $x^i \mapsto \zeta_n^i$). This is an example of a character.

- If K and F are two fields and $\phi : K \to F$ is a field map, then ϕ restricts to a character $\phi' : K^\times \to F^\times$.

Note that the set $\mathrm{Fun}(G, F)$ of all functions from G to F is an F-vector space and that the characters f G are elements of this vector space. Therefore it makes sense to talk about linear independence for sets of characters. A point to observe here is that arbitrary linear combinations $\sum_i l_i\chi_i$ are not, in general, group homomorphisms.

Definition 4.70. For G and F and characters $\chi_1, \ldots, \chi_n$, we say these characters are *linear independent* if whenever $\sum_{i=1}^n l_i\chi_i = 0$ (the constant map 0), we must have $l_i = 0$ for all i. Making this even more explicit: $\chi_1, \ldots, \chi_n$, are linear independent if given $l_i \in F$ such that $\sum_{i=1}^n l_i\chi_i(g) = 0$ for all $g \in G$, we must have $l_i = 0$ for all i.

Theorem 4.71 (Linear Independence of Characters)**.** *Let G be a group, let F be a field, and let $\chi_j : G \to F^\times$, $j = 1, \ldots, m$ be any finite list of distinct characters (i.e., for all $i \neq j$, we have $\chi_i(g) \neq \chi_j(g)$ for at least one $g \in G$). Then $\chi_1, \ldots, \chi_m$ are linearly independent.*

The Theorem is sort of a "Sophomore's dream", since it is saying that if a list of a certain sort of vectors in a certain vector space has no repetitions, then the vectors are linearly independent.

Proof. We proceed by induction on m.

The case $m = 1$ is clear since $\chi_1(g) \neq 0$ for all g implies that $l_1\chi_1(g) = 0$ iff $l_1 = 0$.

Suppose $m > 1$ and that $\sum_{i=1}^m l_i\chi_i(g) = 0$ for all $g \in G$ for some $l_i \in F$.

Suppose

$$\sum_{i=1}^m l_i\chi_i = 0 \tag{4.2.2}$$

Evaluating (4.2.2) at hg for $g, h \in G$ and using that χ_i's are group homomorphisms gives

$$0 = \sum_{i=1}^m l_i\chi_i(hg) = \sum_{i=1}^m l_i\chi_i(h)\chi_i(g) \quad \forall g, h \in G. \tag{4.2.3}$$

Multiplying (4.2.2) by $\chi_1(h)$ gives

$$0 = \chi_1(h)\left(\sum_{i=1}^m l_i\chi_i(g)\right) \quad \forall g, h \in G. \tag{4.2.4}$$

Subtracting (4.2.3) from (4.2.4) we get we get

$$0 = \chi_1(h)\left(\sum_{i=1}^m l_i\chi_i(g)\right) - \sum_{i=1}^m l_i\chi_i(h)\chi_i(g) = \sum_{i=2}^m \left(\chi_1(h)l_i - \chi_i(h)l_i\right)\chi_i(g) \quad \forall g, h \in G.$$

Fixing h, the equation above gives a linear dependence between $\chi_2, \ldots, \chi_m$. Using the induction hypothesis we conclude that

$$\chi_1(h)l_i - \chi_i(h)l_i = 0 \quad \forall h \in G$$

for all i, including $i = m$. Since $\chi_1(h) \neq \chi_m(h)$, we get $l_m = 0$, and hence (4.2.2) reduces to

$$\sum_{i=1}^{m-1} l_i \chi_i(g) = 0, \quad \forall g \in G.$$

Using the induction hypothesis again it follows that $l_i = 0$ for all i. □

Example. Let $G = C_n$, generated by x, and define

$$\chi_j : G \to \mathbb{C}$$

for $j = 0, \ldots, n-1$ by $\chi_i(x) = \zeta_n^j = e^{2\pi j/i}$. Clearly these are distinct and hence they must be linearly independent.

We now restate Artin's theorem:

Theorem (Artin's Theorem)**.** *Let L be any field and G any finite subgroup of* $\mathrm{Aut}(L)$*. Then L^G is a subfield of L, L/L^G is a finite Galois extension and* $\mathrm{Gal}(L/L^G) = G$*.*

I will leave it as an exercise to verify the following

Exercise 4.72. Let L be any field and $G \leq \mathrm{Aut}(L)$. Then L^G is a subfield of L.

Proof of Artin's Theorem. Let G be a finite subgroup of $\mathrm{Aut}(L)$ for a field L.

We need to prove L/L^G is a finite extension and that $[L : L^G] = |\mathrm{Aut}(L/L^G)|$.

We start by observing that it suffices to show $[L : L^G] = |G|$. For granting this holds, then clearly L/L^G is a finite extension. Also, $G \leq \mathrm{Aut}(L/L^G)$ is evident from the definitions, and so we would conclude that $|\mathrm{Aut}(L/L^G)| \geq [L : L^G]$. But $|\mathrm{Aut}(L/L^G)| \leq [L : L^G]$ holds for any finite extension by Theorem 4.57.

It remains to prove $[L : L^G] = |G|$.

Let $n = |G|$ and let $G = \{\sigma_1, \ldots, \sigma_n\}$ with $\sigma_1 = \mathrm{id}_L$ being the identity element.

We know by Theorem 4.57 that $[L : L^G] \geq n$ and we want to show that equality holds. If $[L : L^G] > n$, we can find $n+1$ L^G-linearly independent elements $\omega_1, \ldots, \omega_{n+1}$ in L. Consider the system of n equations with $n+1$ unknowns

$$\begin{aligned}
\sigma_1(\omega_1)x_1 + \cdots + \sigma_1(\omega_{n+1})x_{n+1} &= 0 \\
\sigma_2(\omega_1)x_1 + \cdots + \sigma_2(\omega_{n+1})x_{n+1} &= 0 \\
&\vdots = \vdots \\
\sigma_n(\omega_1)x_1 + \cdots + \sigma_n(\omega_{n+1})x_{n+1} &= 0.
\end{aligned}$$

Since there are fewer equations then unknowns, this system has a non-trivial solution. Among these, choose the solution that has the least number r of non-zero components;

by reordering the ω's we may assume this solution has the form $(a_1, \ldots, a_r, 0, \ldots, 0)$ with $a_i \neq 0$ for all i. By scaling, we may assume $a_r = 1$. If all the a_i's belong to L^G then (since $\sigma_1 = \mathrm{id}_G$), the first row contradicts the linear indepdence of the ω's. Reordering again, we may assume $a_1 \notin L^G$. (Note that, in particular, this shows $r > 1$.) We thus have the system

$$\begin{aligned}
\sigma_1(\omega_1)a_1 + \cdots + \sigma_1(\omega_{r-1})a_{r-1} + \sigma_1(\omega_r) &= 0 \\
\sigma_2(\omega_1)a_1 + \cdots + \sigma_2(\omega_{r-1})a_{r-1} + \sigma_2(\omega_r) &= 0 \\
&\vdots \\
\sigma_n(\omega_1)a_1 + \cdots + \sigma_n(\omega_{r-1})a_{r-1} + \sigma_n(\omega_r) &= 0
\end{aligned}$$

Now, since $a_1 \notin L^G$, there is a k with $\sigma_k(a_1) \neq a_1$. Apply σ_k to the j-th row to obtain

$$\sigma_k\sigma_j(\omega_1)\sigma_k(a_1) + \cdots + \sigma_k\sigma_j(\omega_{r-1})\sigma_k(a_{r-1}) + \sigma_k\sigma_j(\omega_r) = 0$$

Since G is a group, as j ranges over all possibilities, $\sigma_k\sigma_j$ ranges over all elements of G. Thus

$$\sigma_i(\omega_1)\sigma_k(a_1) + \cdots + \sigma_i(\omega_n)\sigma_k(a_{r-1}) + \sigma_i(\omega_r) = 0 \quad 1 \leq i \leq n.$$

For each i, subtracting this equation for the i-th equation in the previous system yields

$$\sigma_i(\omega_1)(a_1 - \sigma_k(a_1)) + \cdots + \sigma_i(\omega_{r-1})(a_{r-1} - \sigma_k(a_1)) = 0 \quad 1 \leq i \leq n.$$

Since $a_1 - \sigma_k(a_1) \neq 0$, this is a non-trivial solution with fewer than r non-zero components, a contradiction. □

April 19, 2019

We now prove a few useful corollaries of Artin's Theorem.

Corollary 4.73. *Let L/F be any finite Galois extension. Then $F = L^{\mathrm{Gal}(L/F)}$.*

Proof. Note that $F \subseteq L^{\mathrm{Gal}(L/F)}$ holds by definition, and so

$$[L : F] = [L : L^{\mathrm{Gal}(L/F)}][L^{\mathrm{Gal}(L/F)} : F]$$

by the degree formula. But Artin's Theorem gives that $[L : L^{\mathrm{Gal}(L/F)}] = |\mathrm{Gal}(L/F)|$ and we also know that $[L : F] = |\mathrm{Gal}(L/F)|$. Thus $[L^{\mathrm{Gal}(L/F)} : F] = 1$ and thus we have $F = L^{\mathrm{Gal}(L/F)}$. □

Example. We know from before that $L = \mathbb{Q}(\sqrt[4]{2}, i)$ is Galois over $\mathbb{Q}$ with Galois group D_8. More precisely, this identification is given by letting $\alpha_1 = \sqrt[4]{[2]}$, $\alpha_2 = i\sqrt[4]{2}$, $\alpha_3 = -\sqrt[4]{2}$, $\alpha_4 = -i\sqrt[4]{2}$ and labelling the four corners of a square with $\alpha_1, \ldots, \alpha_4$, counter-clockwise. Consider $\beta := \alpha_1 + \cdots \alpha_4$ and $\gamma = \alpha_1 \cdots \alpha_4$. Then each of β and γ are fixed by every Galois automorphism and hence, by the previous Corollary, each must be rational. In fact, one can easily see that $\beta = 0$ and $\gamma = 2$, but notice that the exact same reasoning would apply in general to the sum of roots and the product of roots in the splitting field of any separable polynomial.

Corollary 4.74. *Suppose L/F is a Galois extension. For every $\alpha \in L$, $m_{\alpha,F}(x)$ is separable and all of its roots belong to L.*

Proof. Pick any element $\alpha \in L$ and consider the orbit $\alpha = \alpha_1, \ldots, \alpha_m$ of α under the action of $\mathrm{Gal}(L/K)$. Set

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_m).$$

For any $\tau \in \mathrm{Gal}(L/F)$ we have

$$f^\tau(x) = (x - \tau(\alpha_1)) \cdots (x - \tau(\alpha_m)) = f(x)$$

since τ permutes the elements of any orbit. This proves that $f(x)$ has all its coefficients in the field $F^{\mathrm{Gal}(L/F)}$, which by the previous corollary coincides with the field F. Thus $f(x) \in F[x]$. Moreover it is clear by construction that $f(x)$ is separable. Since α is a root of $f(x)$, $m_{\alpha,F}(x)$ divides $f(x)$, and thus it too is separable and has all its roots in L. □

Exercise 4.75. In fact, referring to the notation of the proof, we have $f(x) = m_{\alpha,F}(x)$. (This is a homework problem)

Finally, a corollary that we have stated before which shows that Galois extensions are the same as splitting fields of separable polynomials.

Corollary 4.76. *A finite field extension L/F is Galois if and only if it is the splitting field of some separable polynomial $f(x) \in F[x]$ with coefficients in F.*

Proof. We proved before that if L is the splitting field of some separable polynomial $f(x) \in F[x]$, then L/F is Galois. For the other direction, let $\beta_1, \ldots, \beta_n \in L$ be any elements so that $L = F(\beta_1, \ldots, \beta_n)$. (For example, the β_i's could be chosen to be a F-basis of L.) Set $g(x) = \prod_{i=1}^n m_{\beta_i,F}(x)$. By the previous Corollary, $g(x)$ is separable and all of this roots belong to L, and hence the splitting field of g is contained in L. Since β_i is a root of $g(x)$ for all i, L must be precisely the splitting field of $g(x)$. □

Proof of the Fundamental Theorem of Galois Theory 4.67. Both functions are well-defined. (For example, for each E, we know from above that L/E is Galois and hence writing $\mathrm{Gal}(L/E)$ is justified.) We check that both ways of composing them give the identity:

Given a subgroup H of $\mathrm{Gal}(L/F)$, we have $\mathrm{Gal}(L/L^H) = H$ by Artin's Theorem. Given an intermediate field E, L/E is Galois by Corollary 4.65 and hence $L^{\mathrm{Gal}(L/E)} = E$ by Corollary 4.73. This establishes the bijective correspondence.

For brevity, set $G = \mathrm{Gal}(L/F)$. We verify the itemized list of properties:

1. That the correspondence is order reversing is immediate from the definitions.

2. For any subgroup $H \leq G$, by Artin's Theorem $[L : F] = |G|$ and $[L : L^H] = |H|$ and hence, using the degree formula, we have

$$[L^H : F] = \frac{[L : F]}{[L : L^H]} = \frac{|G|}{|H|} = [G : H].$$

3. This one is the most interesting one. Suppose E is an intermediate field that is Galois over F. For $\sigma \in G$ and $\alpha \in E$, set $f(x) = m_{\alpha,F}(x) \in F[x]$. Since $\sigma(\alpha)$ is also a root of $f(x)$ and E/F is Galois, by Corollary 4.74 we have that $\sigma(\alpha) \in E$ too. Suppose now $\tau \in \mathrm{Gal}(L/E)$. For any $\alpha \in E$ we have $\sigma^{-1}(\tau(\sigma(\alpha)) = \sigma^{-1}(\sigma(\alpha)) = \alpha$ since $\sigma(\alpha) \in E$. This proves that $\sigma^{-1}\tau\sigma \in \mathrm{Gal}(L/E)$ and hence that $\mathrm{Gal}(L/E) \trianglelefteq G$. We have shown that if E is Galois over F, then the corresponding subgroup $\mathrm{Gal}(L/E)$ of G is normal.

   For the converse, suppose $N \trianglelefteq G$ and let $E = L^N$, so that $N = \mathrm{Gal}(L/E)$. We prove E is the splitting field over F of a separable polynomial and hence is Galois over F.

   Pick any $\alpha \in E$ and set $f(x) = m_{\alpha,F}(x)$. By Corollary 4.74, $f(x)$ is separable and all of its roots belong to L. I claim that all the roots must in fact belong to E. Let $\beta \in L$ be any other root of $f(x)$. Since $f(x)$ is irreducible and L/F is Galois, G acts transitively on the set of roots of $f(x)$ (see Lemma below). Thus, there is a $\sigma \in G$ with $\sigma(\alpha) = \beta$. Since N is normal, for any $\tau \in N$ we have $\sigma\tau' = \tau\sigma$ for some $\tau' \in N$. Applying this to $\alpha \in E$ gives

$$\beta = \sigma(\alpha) = \sigma\tau'(\alpha) = \tau\sigma(\alpha) = \tau(\beta)$$

   which shows that β is fixed by N. But then $\beta \in E = L^N$.

   We have proven that for each $\alpha \in E$, E contains the splitting field of the separable polynomial $m_{\alpha,F}(x)$. We have $E = F(\alpha_1, \ldots, \alpha_l)$ for some $\alpha_1, \ldots, \alpha_l \in E$. It follows that E is the splitting field of the separable polynomial $\prod_i m_{\alpha_i,F}(x)$.

4. It remains to prove that if $E = L^N$ with N normal then $\mathrm{Gal}(E/F)$ is isomorphic to G/N. For each $\sigma \in G$, I claim that $\sigma(E) \subseteq E$. To see this, given $\alpha \in E$, $\sigma(\alpha)$ is also a root of $m_{\alpha,F}(x)$. But since E/F is Galois, it must contain all of the roots of this polynomial.

   We thus have that the restriction of σ to E determines a field map $\sigma|_E : E \hookrightarrow E$ which because it is injective must in fact be an automorphism. We thus have a well-defined function

$$\phi : G \to \mathrm{Gal}(E/F)$$

   given by $\phi(\sigma) = \sigma|_E$, and it is clearly a group homomorphism. The kernel is clearly N and hence we have an induced injective group homomorphism

$$\overline{\phi} : G/N \hookrightarrow \mathrm{Gal}(E/F).$$

   But $|N| = |\mathrm{Gal}(E/F)|$ by (2) and so this map must be an isomorphism.

□

April 22, 2019

4.2.4 The primitive element theorem

The last topic I want to discuss in detail this semester is the Primitive Element Theorem. Here is the statement:

Theorem 4.77 (Primitive Element Theorem)**.** *If L/F is finite and separable then L is simple, i.e. $L = F(\theta)$. In particular, if L/F is a finite extension of fields of characteristic zero, then L is simple.*

Definition. Recall that an element θ so that $L = F(\theta)$ is a *simple extension* is called a *primitive element* for the extension L/F.

Lemma 4.78. *If L/F is a finite extension with F infinite, then $L = F(\theta)$ if and only if there are only finitely many subfields of L containing F.*

Proof. First we show if there are only finitely many subfields of L containing F then L is simple. It's sufficient to show $F(\alpha, \beta)$ is simple for any $\alpha, \beta \in L$ and then the statement about L will follow by induction on the dimension of L. Consider the intermediate fields $E_c = F(\alpha + c\beta)$ for $c \in F$. Since there are only finitely many intermediate subfields, but infinitely many $c \in F$ we have

$$F(\alpha + c\beta) = F(\alpha + c'\beta) =: E \text{ for some } c \neq c'.$$

Then $\alpha + c\beta - (\alpha + c'\beta) = (c - c')\beta \in E$, so $\beta \in E$ and similarly $\alpha \in E$, thus $E = F(\alpha + c\beta) = F(\alpha, \beta)$.

For the converse, suppose $L = F(\theta)$ is simple and let $f(x) = m_{\theta,F}(x)$. Let E be an intermediate field and $g(x) = m_{\theta,E}(x)$. Then $g(x) \mid f(x)$ in $E[x]$, so $g(x)$ is an irreducible factor of $f(x)$. Consider E' to be the field obtained by adjoining the coefficients of $g(x)$ to F. Since $g(x) = m_{\theta,E}(x) = m_{\theta,E'}(x)$, we have $[F(\theta) : E] = [F(\theta) : E'] = \deg(g(x))$ and since $E' \subseteq E$ the degree formula gives $E = E'$. So all intermediate fields are generated by the coefficients of the irreducible factors of $f(x)$. □

We need one more notion before we can proceed.

Definition 4.79. Let L/F be a finite separable extension. The *Galois closure* of L over F is the smallest (w.r.t. containment) Galois extension of F containing L, i.e.

$$L^{\text{Gal}} = \bigcap_{K/F \text{ Galois}, F \subseteq L \subseteq K} K.$$

Remark 4.80. Given a finite separable extension L/F there is always a Galois extension K/F such that $F \subseteq L \subseteq K$. For example, one can pick a basis $\{\beta_1, \ldots, \beta_n\}$ for L over F and take K to be the splitting field of the product of the minimal polynomials of $\beta_1, \ldots, \beta_n$. Then K/L will be the splitting field of a separable polynomial, hence Galois.

This shows that the set indexing the intersection above is not empty, so the Galois closure exists as defined.

Using this, we can prove the Primitive Element Theorem.

Proof of the Primitive Element Theorem 4.77. If F is a finite field and hence so is L, then L is automatically primitive over any subfield. Indeed, since L is finite $(L^\times, \cdot)$ is cyclic by a homework problem. Let θ be a generator for this multiplicative group, then $L = F(\theta)$.

The remaining case that needs to be addressed is when F is infinite. Let K be the Galois closure of L over F. Then $G = \mathrm{Gal}(K/F)$ is finite and has finitely many subgroups, thus by the Galois correspondence there are finitely many subfields of K (hence also of L) containing F. By the previous Lemma it follows that L is simple. □

Cutoff for final.

April 24, 2018

4.2.5 Solvable polynomials and solvable groups

We next talk about the Galois groups of the splitting field of polynomials of the form $x^n - a$. There are two main calculations: the case when $a = 1$ and the case where $a \neq 1$ and the ground field already contains all the n-th roots of unity.

These calculations will be used to prove what Galois himself sort-of proved: if the roots of a polynomial can be expressed using "iterated radicals",then the Galois group of its splitting field must be a solvable group.

Definition 4.81. A primitive n-th root of 1 over an arbitrary field F is an element ζ in the splitting field K of $x^n - 1$ over F (or in the algebraic closure $\overline{F}$) such that ζ generates the (multiplicative) subgroup

$$\mu_n(K) := \{\alpha \in K \mid \alpha^n = 1\} \leq (K^\times, \cdot),$$

Remark 4.82. Recall that for every field K, every finite subgroup of $K^\times$ is cyclic. In particular, $\mu_n(K)$ is a cyclic group.

Remark 4.83. Note that if $\mathrm{char}(L) \nmid n$, the polynomial $x^n - 1$ is separable, since its derivative is nx^{n-1} and hence $\gcd(nx^{n-1}, x^n - 1) = 1$. In this case $|\mu_n(K)| = n$ and so

$$\mu_n(K) = \{1, \zeta, \zeta^2, \ldots, \zeta^{n-1}\}.$$

However if $\mathrm{char}(L) \mid n$ then $\mu_n(K)$ can have fewer than n elements. For example the polynomial $x^2 - 1 = (x-1)^2$ has a unique root over any field F of characteristic 2 and in this case the unique 2-nd root of 1 is 1.

Example. For $F = \mathbb{Q}$, a primitive n-th root of unity is $e^{2\pi i/n} \in \overline{\mathbb{Q}}$. So is $e^{2\pi ij/n}$ for any j with $\gcd(n, j) = 1$.

Theorem 4.84. *Let F be a field and n a positive integer with* $\mathrm{char}(F) \nmid n$*, and let $\zeta \in \overline{F}$ be a primitive n-th root of unity. The extension $F \subseteq F(\zeta)$ is finite Galois and the Galois group* $\mathrm{Gal}(F(\zeta)/F)$ *is isomorphic to a subgroup of $(\mathbb{Z}/n)^\times$. In particular,* $\mathrm{Gal}(F(\zeta)/F)$ *is an abelian group.*

Proof. By definition, $F(\zeta)$ contains all the roots of $x^n - 1$ and thus is the splitting field of it over F. As observed above, the polynomial $x^n - 1$ is separable, and thus $F(\zeta)/F$ is Galois.

For $\sigma \in \mathrm{Gal}(F(\zeta)/F)$ we have $\sigma(\zeta)$ is also and n-th root of unity, since $\sigma(\zeta)^n = \sigma(\zeta^n) = \sigma(1) = 1$. Moreover, we claim that $\sigma(\zeta)$ must also be a primitive n-th root of unity. For notice that since $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$ are distict, so too are $1, \sigma(\zeta), \sigma(\zeta)^2, \ldots, \sigma(\zeta)^{n-1}$ since $\sigma(\zeta^l) = \sigma(\zeta)^l$ for all l.

This proves that $\sigma(\zeta) = \zeta^j$ for an integer j (unique modulo n) such that $\gcd(j, n) = 1$. Thus we have a well-defined function

$$\Phi : \mathrm{Gal}(F(\zeta)/F) \to (\mathbb{Z}/n)^\times$$

given by $\Phi(\sigma) = j$, where j satisfies $\sigma(\zeta) = \zeta^j$.

If σ' is another element of $\mathrm{Gal}(F(\zeta)/F)$ and $\sigma'(\zeta) = \zeta^{j'}$, then we have

$$(\sigma' \circ \sigma)(\zeta) = \sigma'(\zeta^j) = \sigma'(\zeta)^j = \zeta^{j'j}.$$

This proves htat $\Phi(\sigma' \circ \sigma) = \Phi(\sigma') \cdot \Phi(\sigma)$; i.e., Φ is a group homomorhism.

If $\Phi(\sigma) = 1$, then σ fixes ζ and hence must be the trivial autmorphism. This shows Φ is one-to-one. □

Corollary 4.85. $\mathrm{Gal}(\mathbb{Q}(e^{2\pi i/n})/\mathbb{Q}) \cong (\mathbb{Z}/n)^\times$ *via the map construction in the proof of Theorem 4.84*

Proof. We know there is an injective homormophism $\mathrm{Gal}(\mathbb{Q}(e^{2\pi i/n}/\mathbb{Q}) \hookrightarrow (\mathbb{Z}/n)^\times$. Because the degree of the minimal polynomial of $e^{2\pi i/n}$, $\deg(\Phi_n) = \phi(n)$ implies that $|\mathrm{Gal}(\mathbb{Q}(e^{2\pi i/n}/\mathbb{Q})| = \phi(n) = |(\mathbb{Z}/n)^\times|$ this homomorphism must be onto. □

We now cover the Galois groups of polynomials of the form $x^n - a$ in the case where the base field contains all the n-th roots of unity.

Theorem 4.86. *Given a field F, an element $a \in F$ and a positive integer n such that* $\mathrm{char}(F) \nmid n$ *and F contains a primitive n-th root of unity, let L the splitting field of $x^n - a$ over F. Then L/F is finite Galois and* $\mathrm{Gal}(L/F)$ *is isomorphic to a subgoup of $\mathbb{Z}/n$ and hence it is cyclic.*

Proof. If $a = 0$, $L = F$ and the result is trivially true.

If $a \neq 0$, then $\gcd(x^n - a, nx^{n-1}) = 1$ and hence $x^n - a$ is separable.

Let α be any one root of $x^n - a$ in L and let $\zeta \in F$ be the primitive n-th root of unity. Then $\zeta^j \alpha$, $j = 0, \ldots, n-1$, give all the roots of $x^n - a$. (Note that they are

distinct.) In particular, $L = F(\alpha)$. Also, for each $\sigma \in \mathrm{Gal}(L/F)$, we have $\sigma(\alpha) = \zeta^j \alpha$, with j well-defined modulo n. Define

$$\Psi : \mathrm{Gal}(L/F) \to \mathbb{Z}/n$$

by $\Psi(\sigma) = j$ with j defined to be the interger (unique module n) that satisfies $\sigma(\alpha) = \zeta^j \alpha$. If $\sigma'(\alpha) = \zeta^{j'} \alpha$, then

$$(\sigma' \circ \sigma)(\alpha) = \sigma'(\zeta^j \alpha) = \zeta^j \zeta^{j'} \alpha = \zeta^{j+j'} \alpha.$$

(Note that we used that $\zeta \in F$ and hence that it is fixed by σ'.) This proves Ψ is a group homorphism. It is injective since $\Psi(\sigma) = 0$ implies that σ fixes α and hence all of L. □

Definition 4.87. For a field F of characeteristic 0, we say $f(x) \in F[x]$ is *solvable by radicals over* F if there exists a finite chain of field extensions

$$F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_m$$

such that $f(x)$ splits completely in F_m (in other words, F_m contains the splitting field of $f(x)$) and for each i the field extension $F_i \subseteq F_{i+1}$ is the splitting field of an polynomial of the form $x^{n_i} - a_i$ for some positive integer n_i and some element $a_i \in F_i$.

It should be pointed out that $a_i = 1$ is allowed here, so that some of the steps in this definitions may involve adjoining n-th roots of unity.

Roughly speeking $f(x)$ is solvable by radicals if each of its roots can be written by a, perhaps extremely complicated, expression involving sums, products and iterated n-th roots of elements of F.

Example. $f(x) = x^4 + bx^2 + c \in \mathbb{Q}[x]$ is solvable by radicals over $\mathbb{Q}$ since its roots are

$$\pm\sqrt{\frac{-b \pm \sqrt{b^2 - 4c}}{2}}.$$

Explicitly, we could set F_1 to be the splitting field of $x^2 - (b^2 - 4c)$ over $\mathbb{Q}$, F_2 to be the spliting field of $x^2 - \left(\frac{-b+\sqrt{b^2-4c}}{2}\right)$ over F_1, and F_3 to be the spliting field of $x^2 - \left(\frac{-b-\sqrt{b^2-4c}}{2}\right)$ over F_2. (I am not sure if $F_3 = F_2$ or $F_3 \subset F_2$, but either way the tower I have given shows that $f(x)$ is solvable by radicals.)

April 26, 2019

The notion of solvable polynomial has a group theoretic counterpart.

Definition 4.88. A group G is called *solvable* of it has a sequence of subgroups $\{e\} = N_0 \trianglelefteq N_1 \trianglelefteq \ldots \trianglelefteq N_k = G$ for some such that for all $0 \leq i \leq k-1$ $N_i \trianglelefteq N_{i+1} \leq G$ and the quotient groups N_{i+1}/N_i are abelian.

It turns out that there is a close relationship between solvable groups and solvable polynomials.

Theorem 4.89. *Assume F is a field of characteristic 0.*[1] *If $f(x) \in F[x]$ is solvable by radicals, then the Galois group of the splitting field of $f(x)$ over $F[x]$ is a solvable group.*

Sketch of proof. For a suitable n, we may assume there is a tower

$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_m$$

such that $L \subseteq F_m$, F_1 is the splitting field over F of $x^n - 1$ for some n, and that, for each $i \geq 1$, F_{i+1} is the splitting field over F_i of a polynomial of the form $x^d - a$ such that $a \in F_i$ and $d \mid n$. Note that $d \mid n$ means that F_i contains all the d-th roots of 1, and thus Theorem 4.86 applies to the extension F_{i+1}/F_i for each $i \geq 1$.

It turns out that there is an extension E such that

$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_m \subseteq E$$

and E/F is Galois with a chain of normal subgroup inclusions

$$\mathrm{Gal}(E/F_m) \trianglelefteq \mathrm{Gal}(E/F_{m-1}) \trianglelefteq \mathrm{Gal}(E/F_{m-2}) \trianglelefteq \cdots \trianglelefteq \mathrm{Gal}(E/F_1) \trianglelefteq \mathrm{Gal}(E/F)$$

The key point is that by Theorems 4.84 and 4.86, the groups

$$\mathrm{Gal}(F_{i+1}/F_i) \cong \mathrm{Gal}(E/F_i)/\mathrm{Gal}(E/F_{i+1}) \text{ for } i = 0, \ldots, m-1$$

are all abelian. I claim that these properties imply that $\mathrm{Gal}(E/F)$ is a solvable group and in turn this implies that $\mathrm{Gal}(L/F)$ is solvable. □

Corollary 4.90. *If $f(x) \in \mathbb{Q}[x]$ is any 5-th degree, irreducible polynomial with exactly 3 real roots, then $f(x)$ is not solvable by radicals.*

Proof. Let L be the splitting field of $f(x)$. By the Theroem, it suffices to prove $\mathrm{Gal}(L/\mathbb{Q})$ is not a sovlable gorup. In fact we show it is isomorphic to S_5.

Let $\alpha_1, \alpha_2, \alpha_3$ be the three real roots of $f(x)$ and let α_4, α_5 the two complex ones. Note that $\overline{\alpha_4} = \alpha_5$. Using this ordering of the roots we identify $\mathrm{Gal}(L/\mathbb{Q})$ as a subgroup of S_5.

Let $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ denote complex conjugation — it corresponds to the transposition $(4, 5) \in S_5$. Since $[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = 5$ we have $5 \mid |\mathrm{Gal}(L/\mathbb{Q})|$. Since 5 is prime, there is an element $\tau \in \mathrm{Gal}(L/K)$ of order 5 by Cauchy's Theorem. Such an element is necessarily a 5-cycle. The result follows since any 5-cycle and any transposition necessarily generate all of S_5 (exercise).

Finally notice that S_5 is not solvable, since, as proven in math 817, the only nontrivial normal subgroup of S_5 is A_5 and A_5 has no nontrivial normal subgroups. Hence the only possible composition series for S_5 would be $H_0 = \{e\} \leq A_5 \leq S_5$, but in this series the quotient $A_5/\{e\} \cong A_5$ is not abelian. □

[1] $\mathrm{char}(F) = 0$ is not a necessary assumption, but I included it to make both the statement and the proof simpler.

Example. The polynomial $f(x) = x^5 - 4x + 2$ is not solvable by radicals over $\mathbb{Q}$. It is irreducible in $\mathbb{Q}[x]$ by Eisentstein. Moreover, $f'(x) = 5x^4 - 4$ has precisely two roots and changes signs at these roots. It follows that $f(x)$ must have exactly 3 real roots.

Finally, I mention that the converse of Theorem 4.89 is also true: (At least in characteristic 0) if the Galois group of $f(x)$ is solvable, then $f(x)$ is solvable by radicals. Since S_4 is solvable, it follows that every polynomial of degree at most 4 is solvable by radicals. Indeed, formulas for the roots of degree 2, 3 and 4 polynomials have been known for hundreds of years, and they involve only sums, products, quotients and square, cube and fourth roots.

Example. The group S_4 is solvable because of the following sequence of subgroups

$$\{e\} \trianglelefteq V \trianglelefteq A_4 \trianglelefteq S_4,$$

where $V = \{e, (12)(34), (14)(23), (13)(24)\}$, where V is abelian (as any group of order 4 is) and the quotients S_4/A_4 and A_4/V are abelian as well since they have order 2.