

1 Groups

[2]**Definition 1:** A binary operation on a set G is a function $\star : G \times G \rightarrow G$. We write $a \star b$ for $\star(a, b)$. A binary operation is associative if for all $a, b \in G$, we have $(a \star b) \star c = a \star (b \star c)$, and commutative if for all $a, b \in G$, $a \star b = b \star a$.

[1]**Lemma 2: (Generalized Associativity Law)** For an associative binary operation, $a_1 \star a_2 \star \dots \star a_n$ gives the same value no matter how the parentheses are placed.

[2]**Definition 3:** A (two-sided) identity for \star is an element $e \in G$ so that for all $a \in G$, $a \star e = e \star a = a$.

[1]**Lemma 4:** Identities are unique.

[2]**Definition 5:** A group is a set G and a binary operation \star on G , represented as (G, \star) , such that

1. (Associative) For all $a, b, c \in G$, we have $(a \star b) \star c = a \star (b \star c)$.
2. (Identity) There exists $e \in G$ such that for all $a \in G$, $a \star e = e \star a = a$.
3. (Inverse) For every $a \in G$ there is some $b \in G$ such that $a \star b = b \star a = e$. Any such $b \in G$ is called an inverse for a .

[1]**Lemma 6:**

1. Inverses are unique.
2. $(a^{-1})^{-1} = a$.
3. $(a \star b)^{-1} = b^{-1} \star a^{-1}$.

[1]**Example 7:** The following are all groups

1. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, and $(\mathbb{C}, +)$.
2. $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, and $(\mathbb{C} \setminus \{0\}, \cdot)$.
3. If $(V, +, \cdot)$ is a vector space, then $(V, +)$ is a group.
4. Consider a tiling of the plane. The set of all isometries of the plane that map tiles to tiles under the binary operation of composition is a group.
5. Given (A, \star) and (B, \diamond) , we make a new group with the set $A \times B$ and an operation $*$ defined by $(a, b) * (c, d) = (a \star c, b \diamond d)$.

[1]**Proposition 8:** (Linear Equations Proposition) Let G be a group and $a, b \in G$. The equations $ax = b$ and $ya = b$ have solutions in G and the solutions are unique. Uniqueness is equivalent to the left and right cancellation laws, i.e.

1. If $au = av$, then $u = v$.
2. If $ua = va$, then $u = v$.

[1]**Corollary 9:** Let $a, b \in G$.

1. If $ab = 1$, then $b = a^{-1}$.
2. If $ba = 1$, then $b = a^{-1}$.
3. if $ab = a$, then $b = 1$.

[1]**Definition 10:** Let G be a group. For $x \in G$, we define $|x|$ to be the smallest positive integer so that $x^n = 1$. If there is no such integer, then $|x| = \infty$.

G is always a group unless otherwise stated.

[1]**Lemma 10:** Let $a \in G$.

1. $|a| = 1$ if and only if $a = 1$.
2. For $a \in (\mathbb{R} \setminus \{0\}, \cdot)$, $|-1| = 2$ and $|a| = \infty$ for $a \neq 1, -1$.

Dihedral Groups

[1]**Definition 11:** Let $n \geq 3$. Then D_{2n} represents the group of symmetries of the regular n -gon.

[1]**Definition 12:** In D_{2n} , we represent a clockwise rotation by $\frac{2\pi}{n}$ by r and s represents the flip that switches vertices 1 and 2. So $D_{2n} = \{1, r, r^2, \dots, r^{n-1}, s, sr, sr^2, \dots, sr^{n-1}\}$.

[1]**Lemma 13:** (Properties of D_{2n})

1. $|D_{2n}| = 2n$
2. $s^2 = r^n = 1, rs = sr^{n-1}$
3. $D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{n-1} \rangle$.

[2]**Definition 14:** Let Ω be a nonempty set. Then the group S_Ω , the symmetric group on Ω is the set of all bijections $\sigma : \Omega \rightarrow \Omega$ along with the binary operation of composition. We will write S_n for $\Omega = \{1, \dots, n\}$.

[1]**Lemma 15:**

1. $|S_n| = n!$
2. $S_\Omega \cong S_\Lambda$ provided $|\Lambda| = |\Omega|$.

[1]**Definition 16:** Given a list of r distinct integers, where $1 \leq r \leq n$, say a_1, a_2, \dots, a_r , the associated r -cycle is $\sigma \in S_n$ such that

1. $\sigma(a_i) = a_{i+1 \bmod r}$ for all $1 \leq i \leq r$.
2. $\sigma(b) = b$ for all $b \in \{1, \dots, n\} \setminus \{a_1, \dots, a_r\}$.

[2]**Lemma 17:**

1. The order of a cycle is its length.
2. $(a_1, a_2, \dots, a_n)^{-1} = (a_n, a_{n-1}, \dots, a_2, a_1)$.
3. Disjoint cycles commute.

[2]**Proposition 18:** (Cycle Decomposition of S_n) Every element of S_n can be written as a product of disjoint cycles and, up to order, this product is unique. The algorithm for finding this decomposition is the obvious one.

[1]**Example 19:** (Multiplying non disjoint cycles) Let $\sigma = (1\ 3)(1\ 2)$ and $\tau = (1, 2)(1\ 3)$. Then $\sigma\tau = (1\ 2\ 3)$, but $\tau\sigma = (1\ 3\ 2)$. Thus S_n is nonabelian for $n \geq 3$.

Matrix and Quaternion Groups

[2]**Definition 20:** The invertible $n \times n$ matrices over \mathbb{R} form a group under matrix multiplication called $GL_n(\mathbb{R})$. We can similarly define a set of matrices of \mathbb{Q} and $\mathbb{Z}/p\mathbb{Z}$, where p is prime.

[2]**Definition 21:** The quaternion group, Q_8 , is the set $\{\pm 1, \pm i, \pm j, \pm k\}$, with a binary operation that can be defined by the following facts:

1. It has the partial multiplication table

1	i	j	k
i	1	k	$-j$
j	$-k$	1	i
k	j	$-i$	1

2. The operation also satisfies $(-x)y = -(xy)$.

Homomorphisms/Isomorphisms

[2]**Definition 22:** Let (G, \star) and (H, \diamond) be groups. We call a function $\varphi : G \rightarrow H$ a homomorphism if for all $x, y \in G$

$$\varphi(x \star y) = \varphi(x) \diamond \varphi(y).$$

Henceforth, we will write $\varphi(xy) = \varphi(x)\varphi(y)$.

[1]**Lemma 23:**

1. $\varphi(1_G) = 1_H$
2. $\varphi(x^n) = \varphi(x)^n$ for $n \in \mathbb{Z}$
3. $|\varphi(x)|$ divides $|x|$.

[1]**Example 24:**

1. Let G be $GL_n(\mathbb{R})$ and H be $(\mathbb{R} \setminus \{0\}, \cdot)$. Then $\det : G \rightarrow H$ is a homomorphism defined by $\det(AB) = \det(A)\det(B)$.
2. Let $G = \{1, -1, -i, i\}$ with multiplication as the operation and define $\varphi : G \rightarrow G$ by $\varphi(\pm 1) = \pm 1, \varphi(i) = -i$, and $\varphi(-i) = i$. This is a homomorphism.
3. Let $H = \{1, -1\}$. Define $\Psi : G \rightarrow H$ by $\Psi(1) = 1, \Psi(-1) = \Psi(i) = \Psi(-i) = -1$. This is not a homomorphism as $-1 \cdot i = -i, \Psi(-1)\Psi(i) = 1$, but $\Psi(-i) = -1$.
4. For any groups G and H , we always have the trivial homomorphism $\Psi : G \rightarrow H$ given $\Psi(x) = 0$ for all $x \in G$.
5. Let $G = \langle r | r^6 = 1 \rangle$ and $H = \langle s | s^3 = 1 \rangle$ and define $\varphi : G \rightarrow H$ by $\varphi(r^i) = s^i$. φ is a homomorphism.

[2]**Definition 25:** For groups G and H , we call $\varphi : G \rightarrow H$ an isomorphism if

1. φ is a homomorphism.
2. φ is a bijection.

In this case, we say that G and H are isomorphic, denoted by $G \cong H$.

[1]**Lemma 26:**

1. The identity map from G to G is an isomorphism.
2. If $\varphi : G \rightarrow H$ is an isomorphism, then $\varphi^{-1} : H \rightarrow G$ is an isomorphism.
3. If $\varphi : G \rightarrow H$ and $\Psi : H \rightarrow K$ are isomorphisms, then $\Psi \circ \varphi$ is an isomorphism.
4. \cong is an equivalence relation.

[1]**Example 27:** (Isomorphisms)

1. The map in part 2 of example 24.
2. $\exp : (\mathbb{R}, +) \rightarrow (\mathbb{R}^+, \cdot)$.

[2]**Proposition 28:** Let Ω and Λ be nonempty sets. Then $S_\Omega \cong S_\Lambda$ if and only if $|\Omega| = |\Lambda|$.

[1]**Proposition 29:** Let G be a group with representation and H be a group. Let s_1, \dots, s_m be the generators of G and $r_1, \dots, r_m \in H$. We can define a function $\varphi : G \rightarrow H$ by $\varphi(s_i) = r_i$ for all $1 \leq i \leq m$.

1. Then if φ satisfies the relations on G , φ is extendable to a homomorphism.
2. If H is generated by $\{r_1, \dots, r_m\}$, then φ is surjective.
3. If $|G| = |H| < \infty$, then φ is an isomorphism.

[1]**Example 30:** Consider $D_{40} = \langle r, s \mid r^{20} = s^2 = 1, r^{19}s = sr \rangle$ and $D_{20} = \langle a, b \mid a^{10} = b^2 = 1, a^9b = ba \rangle$. Define $\varphi(r) = a$ and $\varphi(s) = b$. Then

$$\begin{aligned}\varphi(r)^{20} &= a^{20} = (a^{10})^2 = 1, \\ \varphi(s)^2 &= b^2 = 1,\end{aligned}$$

and

$$\varphi(r)^{19}\varphi(s) = a^{19}b = a^{10}a^9b = ba = \varphi(s)\varphi(r).$$

Hence all of the relations are satisfied and φ extends to a homomorphism. Since $\{a, b\}$ generate H , φ is onto. Since $|D_{40}| \neq |D_{20}|$, φ is not one-to-one. In fact, $\varphi(r^{10}) = a^{10} = 1$, but $r^{10} \neq 1$.

[2]**Definition 31:** The free group with m generators is the group represented by $\langle s_1, s_2, \dots, s_m \rangle$.

Group Actions

[2]**Definition 32:** We say a group G acts on a set A if there is a function from $G \times A \rightarrow A$ written $(g, a) \mapsto g \cdot a$ so that

1. For all $g, h \in G$ and all $a \in A$, $(gh) \cdot a = g \cdot (h \cdot a)$.
2. For all $a \in A$, $1 \cdot a = a$.

This is called a left group action.

[2]**Proposition 33:** For each $g \in G$, we can define a function $\sigma_g : A \rightarrow A$ by $\sigma_g(a) = g \cdot a$. Then the following hold

1. $\sigma_g \in S_A$
2. The map from G to S_A that sends g to σ_g is a homomorphism.
3. Every homomorphism $\sigma : G \rightarrow S_A$ gives rise to a group action.

[1]**Example 34:** (Group Actions) Part I

1. $G = \{1, -1\}$, $A = \mathbb{R}$, and $g \cdot a = ga$.
2. $G = GL_n(\mathbb{R})$, $A = M_n(\mathbb{R})$, and $g \cdot a = ga$ (Matrix multiplication)
3. For every group G and any set A , we define the trivial action by $g \cdot a = a$ for all $a \in A$.
4. For a nonempty set A , define an action of S_A on A by applying $g \in S_A$ to $a \in A$. The associated homomorphism from S_A to S_A is the identity.

[1]**Definition 35:** The stabilizer of $a \in A$ is $\{g \in G : g \cdot a = a\}$ and is denoted by G_a . The orbit of $a \in A$ is $\{g \cdot a : g \in G\}$. The kernel of the action is $\{g \in G : \text{for all } a \in A, g \cdot a = a\}$.

[1]**Example 36:** (Group Actions) Part II

1. $G_3 = \{1\}$, $G_0 = \{1, -1\}$, the orbit of 3 is $\{3, -3\}$, the orbit of 0 is $\{0\}$, and the kernel of the action is $\{1\}$.
2. For a invertible, the orbit is $GL_n(\mathbb{R})$ and for each noninvertible $a \in A$, the orbit contains exactly one matrix in reduced row echelon form.
3. There is only 1 orbit, all of A . The stabilizer of a is the elements of S_A that fix a , i.e. the products of cycles without a .

2 Subgroups

[2]**Definition 37:** Given a group G , we call $H \subseteq G$ a subgroup of G if H is nonempty and

1. For all $x \in H$, $x^{-1} \in H$.
2. For all $x, y \in H$, $xy \in H$.

We write $H \leq G$. If $H \neq G$, then we write $H < G$.

[1]**Lemma 38:**

1. The inclusion map $i : H \rightarrow G$ is an injective homomorphism.
2. The identity of H is the identity of G .
3. For $x \in H$, $x^{-1} \in H$ is the same as x^{-1} in G .
4. If $H \leq K$ and $K \leq G$, then $H \leq G$.
5. If $H \leq G$ and $K \leq G$, then $H \cap K \leq G$.
6. If $H_i \leq G$ for all $i \in I$, then $\bigcap_{i \in I} H_i \leq G$.

[1]**Example 39:**

1. $\mathbb{Z} < \mathbb{Q}, \mathbb{Q} < \mathbb{R}, \mathbb{R} < \mathbb{C}$
2. For any group G , $\{1\}$ and G are subgroups. We call $\{1\}$ the trivial subgroup.
3. $\{2n : n \in \mathbb{Z}\} \leq (\mathbb{Z}, +)$.
4. $\{n : n \geq 0\}$ is not a subgroup of $(\mathbb{Z}, +)$.
5. $(\mathbb{Q} \setminus \{0\}, \cdot)$ is not a subgroup of $(\mathbb{R}, +)$.

[2]**Proposition 40:** (Subgroup Criterion) For a group G , $H \subseteq G$ is a subgroup if and only if

- (1) H is nonempty.
- (2) For all $x, y \in H$, $xy^{-1} \in H$.

If H is finite, it suffices to show H is nonempty and for all $x, y \in H$, we have $xy \in H$.

[2]**Definition 41:** Let G be a group and $a \in G$. The centralizer of a in G denoted by $C_G(a)$ is $\{g \in G : gag^{-1} = a\}$.

[1]**Proposition 42:** $C_G(a)$ is a subgroup of G .

[2]**Definition 43:** For any set $A \leq G$. The centralizer of A in G , denoted by $C_G(A)$, is $\{g \in G : gag^{-1} = a \text{ for all } a \in A\}$.

[2]**Definition 44:** The center of G , denoted by $Z(G)$, is $\{g \in G : ga = ag \text{ for all } a \in G\}$, i.e. $C_G(G)$.

[2]**Definition 45:** Define $gAg^{-1} = \{gag^{-1} : a \in A\}$. Then the normalizer of A in G is the set $N_G(A) = \{g \in G : gAg^{-1} = A\}$.

[1]**Lemma 46:**

1. $C_G(A) \leq N_G(A)$
2. $N_G(A) \leq G$

[1]**Example 47:** $N_{D_8}(\{1, r, r^2, r^3\}) = D_8$.

[1]**Proposition 48:** Let G be acting on a set A . The stabilizers of $s \in A$, $G_s(A)$ and the kernel of the action are both subgroups of G .

[1]**Example 49:**

1. For any group G , G acts on itself by conjugation. That is $A = G$ and $g \cdot h = g^{-1}hg$. Then $Z(G)$ is the kernel of this operation.

2. Let A be a subset of G . Then $N_G(A)$ acts on A by conjugation. That is $g \cdot h = g^{-1}ag$. The kernel of this action is $C_G(A)$.
3. Let $\mathfrak{P}(G)$ be the subsets of G and let G act on $\mathfrak{P}(G)$ by conjugation element wise. That is $g \cdot A = \{g^{-1}ag : a \in A\}$. The stabilizer of $A \subseteq G$ is $g \in G$ such that $g \in N_G(A)$.

[2] **Corollary 50:** $N_G(A)$ is a subgroup since stabilizers are subgroups.

3 Cyclic Groups and Subgroups

[2] **Definition 51:** We call a group (or subgroup) G cyclic if there is some $x \in G$ so that $G = \{x^n : n \in \mathbb{Z}\}$. We call x a generator of G .

[1] **Proposition 52:**

1. If x is a generator, so is x^{-1} .
2. Cyclic groups are abelian.

[1] **Example 53:** (All of the Cyclic Groups up to Isomorphism)

1. $\{1, r, r^2, \dots, r^{n-1}\}$ in D_{2n} is cyclic with generators r and r^{n-1} .
2. $(\mathbb{Z}, +)$ is cyclic with generator 1 or -1 .

[2] **Proposition 54:** (Order of Cyclic Groups) If $G = \langle x \rangle$, i.e. G is cyclic with generator x , then $|G| = |x|$. Moreover, if $|G| = n$, then $1, x, \dots, x^{n-1}$ are all distinct and $x^n = 1$. Also if $|G| = \infty$, then $x^i = x^j$ for $i, j \in \mathbb{Z}$ implies $i = j$.

[1] **Proposition 55:** Let G be a group and $x \in G$. If $x^m = 1$ and $x^n = 1$, then $x^d = 1$ when $d = \gcd(m, n)$. In particular, if $x^m = 1$, then $|x|$ divides m .

[1] **Theorem 56:** (Cyclic Group Theorem) Any two cyclic groups of the same order are isomorphic. More specifically,

[1] **Notation:** We use Z_n for the cyclic group of order $n \in \mathbb{N}$. Note $Z_n \cong (\mathbb{Z}/n\mathbb{Z}, +)$.

[2] **Proposition 57:** (Order of Powers in Groups) Let G be a group, $x \in G$, and $a \in \mathbb{Z} \setminus \{0\}$. If $|x| = \infty$, then $|x^a| = \infty$. If $|x| = n$, then $|x^a| = \frac{n}{\gcd(a, n)} = \frac{n}{(a, n)}$. In particular, if a divides n , then $|x^a| = \frac{n}{a}$.

[1] **Proposition 58:** (Generator of Cyclic Groups) Let $H = \langle x \rangle$. If $|x| = \infty$, then x^a is a generator if and only if $a = \pm 1$. If $|x| = n < \infty$, then x^a is the generator if and only if $(a, n) = 1$. So the number of generators of H is $\varphi(n)$, the Euler φ function.

[2] **Theorem 59:** Let H be a cyclic group with generator x . Every subgroup of H is cyclic with generator either 1 or x^d , where d is the smallest positive integer k so that x^k is in the subgroup.

1. If $|H| = \infty$, then $\langle x^a \rangle = \langle x^b \rangle$ if and only if $|a| = |b|$.
2. If $|H| = n$, then $\langle x^a \rangle = \langle x^b \rangle$ if and only if $(a, n) = (b, n)$.

[2] **Corollary 58:** If $|H| = \infty$, then the nontrivial subgroups of H correspond to elements of \mathbb{Z}^+ , via $n \mapsto \langle x^n \rangle$. If $|H| = n$, then the subgroups of H correspond to divisors of n via $a \mapsto \langle x^d \rangle$, where $d = n/a$.

[1] **Definition 59:** Let G be a group and $A \subseteq G$. We define the subgroup generated by A denoted by $\langle A \rangle$ to be

$$\bigcap \{H : H \leq G, A \subseteq H\}.$$

This is a subgroup of G since intersections of subgroups are subgroups.

[1] **Corollary 60:** If $K \leq G$ and $A \subseteq K$, then $\langle A \rangle \leq K$. That is, $\langle A \rangle$ is the smallest subgroup of G containing A .

[1] **Proposition 61:** $\langle A \rangle = \{a_1^{\epsilon_1} a_2^{\epsilon_2} \cdots a_n^{\epsilon_n} : n \in \mathbb{Z}, n \geq 0, \text{ each } a_i \in A, \text{ each } \epsilon_i \in \{1, -1\}\}$.

[1] **Remarks:**

1. We will often assume elements of $\langle A \rangle$ have the form $a_1^{\alpha_1} \cdots a_n^{\alpha_n}$, where $a_i \in \mathbb{Z} \setminus \{0\}$ and $a_i \neq a_{i+1}$ for all $i = 1, \dots, n - 1$.
2. If G is abelian and $A = \{a_1, \dots, a_k\}$, then $\langle A \rangle = \{a_1^{\alpha_1} \cdots a_k^{\alpha_k} : \alpha_i \in \mathbb{Z}\}$. Moreover, if $|a_i| = d_i$ for each $1 \leq i \leq k$, then $|\langle A \rangle| \leq d_1 d_2 \cdots d_k$.

3. WARNING!!! In D_{2n} , consider $a = s$ and $b = sr$. Then $\langle a, b \rangle = D_{2n}$, but $|a| = |b| = 2$. As $|D_{2n}| = 2n$, nothing like the previous estimate holds for nonabelian groups.

4. Consider

$$a = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad b = \begin{pmatrix} 0 & 2 \\ 1/2 & 0 \end{pmatrix}$$

in $GL_2(\mathbb{Q})$. So $a^2 = b^2 = 1$, but ab has infinite order.

Quotient Groups

[2]**Definition 62:** Let $\varphi : G \rightarrow H$ be a group homomorphism. Define the kernel of φ to be $\ker \varphi = \{g \in G : \varphi(g) = 1_H\}$, and the image of φ to be $\text{Im } \varphi = \{h \in H : \exists g \in G \text{ with } \varphi(g) = h\}$.

[1]**Lemma 63:** $\ker \varphi \leq G$ and $\text{Im } \varphi \leq H$.

[1]**Definition 64:** For $\varphi : G \rightarrow H$ a homomorphism with $K = \ker \varphi$, the quotient group of G by K , denoted G/K , is the group with elements $\varphi^{-1}(h)$ for each $h \in H$ and operation $\varphi^{-1}(h_1) \star \varphi^{-1}(h_2) = \varphi^{-1}(h_1 h_2)$ for $h_1, h_2 \in H$.

[1]**Definition 65:** If G is a group and $N \leq G$, then for each $g \in G$, $gN = \{gn : n \in N\}$ is a left coset of N in G . Also, $Ng = \{ng : n \in N\}$ is a right coset of N in G . Any element of a coset is called a representative of that coset. In particular, g is a representative of gN .

[2]**Proposition 66:** Let $\varphi : G \rightarrow H$ be a homomorphism with $\ker \varphi = K$. For each $a \in H$, $\varphi^{-1}(a)$ is a left coset of K in G . Moreover, if $X = \varphi^{-1}(a)$, then for all $u \in X$, $X = uK = Ku$.

[1]**WARNING:** If $K \leq G$ and $u \in G$, it can happen that $uK \neq Ku$. (Being a kernel of a homomorphism is a special thing!)

[2]**Proposition 67:** (Multiplying Cosets) Let $\varphi : G \rightarrow H$ be a homomorphism with kernel K . Then the quotient group operation on left cosets of K in G is given by $uK \star vK = (uv)K$ for $u, v \in G$. In particular, this operation is well-defined.

[1]**Example 68:** Examples of Quotient Groups)

1. Define $\varphi : (\mathbb{Z}, +) \rightarrow Z_n$ by $\varphi(n) = x^n$
2. Let $\varphi : G \rightarrow H$ be a homomorphism. Then if φ is injective, then $G/\{1\} \cong \text{Im } \varphi \cong G$.
3. Let $\varphi : G \rightarrow \{1\}$ be a homomorphism. Then $\ker \varphi = G$ and $G/G \cong \{1\}$.
4. Define $\varphi : (\mathbb{R}^2, +) \rightarrow (\mathbb{R}, +)$ by $\varphi(x, y) = x - y$. Then $K := \ker \varphi = \{(x, x) : x \in \mathbb{R}\}$. Thus $\mathbb{R}^2/K \cong \mathbb{R}$.
5. Consider the Klein 4-Group, $V_4 = \{1, a, b, c\}$ with multiplication table

1	a	b	c
a	1	c	b
b	c	1	a
c	b	a	1

Define $\varphi : Q_8 \rightarrow V_4$ by $\varphi(\pm 1) = 1, \varphi(\pm i) = a, \varphi(\pm j) = b$, and $\varphi(\pm k) = c$. Then φ is a homomorphism and $\ker \varphi = \{\pm 1\}$. So $Q_8/\{\pm 1\} \cong V_4$.

[1]**Proposition 69:** (Cosets Partition) Let $H \leq G$. Then the cosets of H partition G , i.e. $(uH) \cap (vH) \neq \emptyset$ if and only if $uH = vH$. Moreover, if $u, v \in G$, then $uH = vH$ if and only if $v^{-1}u \in H$.

[2]**Proposition 70:** Let $N \leq G$. The operation on left cosets of N given by

$$uN \star vN = (uv)N$$

is well defined if and only if $gng^{-1} \in N$ for all $n \in N$ and $g \in G$. So $N_G(N) = G$. If this is well defined, then the left cosets form a group with this operation and the identity is N and the inverse of gN is $g^{-1}N$.

[2]**Definition 71:** Let $N \leq G$. We call gng^{-1} the conjugate of n by g . We call gNg^{-1} the conjugate of N by g . If $gNg^{-1} = N$, then g normalizes N . We call $N \leq G$ a normal subgroup of G , written $N \trianglelefteq G$, if all elements of G normalize N .

[1]**Theorem 72:** (Characterizations of Normality) Let $N \leq G$. TFAE:

1. $N \trianglelefteq G$.
2. $N_G(N) = G$.
3. $gN = Ng$ for all $g \in G$.
4. The operation $(uN) \cdot (vN) = (uv)N$ is well defined on left cosets of N .
5. $gNg^{-1} \subseteq N$ for all $g \in G$.
6. There is a homomorphism $\pi : G \rightarrow H$ with $\ker \pi = N$.

[1] **Remarks:**

1. For $H \leq G$ and $H \trianglelefteq N_G(H)$ and $N_G(H)$ is the largest subgroup of G with this property.
2. We want to verify normality as easily as possible:
 - (a) If G is abelian, every subgroup is normal.
 - (b) Elements of N always normalize N , so it suffices to check that elements of G/N normalize N . In fact, $N_G(N) \leq G$ so it suffices to verify that the set of coset representatives normalize N . [If $h \in gN$ normalizes N , then for any $n \in N$ hn normalizes N ($N_G(N) \leq N$) and so $gN \subseteq N_G(N)$.
 - (c) It suffices to verify that the generators of G normalize N .
3. To show $gNg^{-1} \subseteq N$, it suffices to show $gng^{-1} \in N$ for all x in a generating set for N .

[1] **Proposition 73:** Let $N \trianglelefteq G$ and $\pi : G \rightarrow G/N$ be the canonical quotient map $\pi(g) = gN$. For a homomorphism $\Psi : G \rightarrow H$, there is a homomorphism $\Phi : G/N \rightarrow H$ such that $\Psi = \Phi \circ \pi$ if and only if $\ker \Psi \supseteq N$.

[1] **Lemma 74:** If G is a group and $H \leq G$, then all cosets of H have the same cardinality.

[2] **Theorem 75:** (Lagrange's Theorem) Let $H \leq G$ and $|G|$ be finite. Then $|H|$ divides $|G|$ and the number of (left) cosets of H in G is $\frac{|G|}{|H|}$.

[1] **Definition 76:** If $H \leq G$, we use $|G : H|$ (or $[G : H]$) for the number of left cosets of H in G . So Lagrange's Theorem says $|G| = |G : H| \cdot |H|$ for finite groups. We call $|G : H|$ the index of H in G .

[1] **Corollary 77:** (Corollaries of Lagrange's Theorem)

1. If $x \in G$ and $|G|$ is finite, then $|x|$ divides $|G|$. In particular, $x^{|G|} = 1$ for all $x \in G$ when G is a finite group.
2. If $|G| = p$, a prime, then $G \cong Z_p$.

[2] **Theorem 78:** (Cauchy's Theorem) If $|G| < \infty$ and a prime p divides $|G|$, then G has an element of order p . (So there is a cyclic subgroup.)

[2] **Theorem 79:** (Sylow's Theorem) If $|G| = p^\alpha m$, where p is prime and $(p, m) = 1$, then G has a subgroup of order p^α .

[1] **Example 80:** (Examples of Non-normal Subgroups)

1. If $H \leq K$ and $K \trianglelefteq G$, then it is not true in general that $H \trianglelefteq G$. In particular, $\langle s \rangle \trianglelefteq \langle s, r^2 \rangle \trianglelefteq D_8$, but $rsr^{-1} = sr^2 \notin \langle s \rangle$, so $\langle s \rangle \not\trianglelefteq D_8$.

[1] **Lemma 81:** If $H \leq G$ and $[G : H] = 2$, then $H \trianglelefteq G$.

Products of Subgroups

[2] **Definition 82:** If $H \leq G$ and $K \leq G$, then $HK = \{hk : h \in H \text{ and } k \in K\}$.

[2] **Proposition 83:** (Product Formula) If $H, K \leq G$ and $|H|$ and $|K|$ are both finite, then $|HK| = \frac{|H||K|}{|H \cap K|}$.

[1] **Example 84:** In S_3 , $H = \langle (1\ 2) \rangle$ and $K = \langle (2\ 3) \rangle$. As $H \cap K = \{1\}$, $|HK| = 4$. As $|S_3| = 6$, $HK \not\leq S_3$ by Lagrange's Theorem. Thus $\langle (1\ 2), (2\ 3) \rangle = S_3$.

[1] **Proposition 85:** If $H, K \leq G$, then $HK \leq G$ if and only if $HK = KH$.

[1] **Proposition 86:** If $H, K \leq G$ and $H \leq N_G(K)$, then $HK \leq G$. In particular, if $K \trianglelefteq G$ and $H \leq G$, then $HK \leq G$.

Isomorphism Theorems

[2]**Theorem 87:** (First Isomorphism Theorem) For $\varphi : G \rightarrow H$ a homomorphism, then $\ker \varphi \trianglelefteq G$ and $\text{Im } \varphi \cong G/\ker \varphi$.

[1]**Corollary 88:**

1. For φ as above, φ is injective if and only if $\ker \varphi = \{1\}$
2. $|G : \ker \varphi| = |\text{Im } \varphi|$

[2]**Theorem 89:** (Second Isomorphism Theorem) Let $A, B \leq G$ with $A \leq N_G(B)$. Then $AB \leq G$, $B \trianglelefteq AB$, $A \cap B \trianglelefteq A$, and $\frac{AB}{B} \cong \frac{A}{A \cap B}$. (Note that A need not be normal in B .)

[2]**Theorem 90:** (Third Isomorphism Theorem) Let $H, K \trianglelefteq G$ with $H \leq K$. Then $K/H \triangleleft G/H$ and $\frac{G/H}{K/H} \cong G/K$.

[2]**Theorem 91:** (Lattice Isomorphism Theorem) Let $N \trianglelefteq G$. For subgroups of G containing N , the map $H \mapsto H/N$ is a bijective correspondence with subgroups of G/N .

[1]**Corollary 92:** If $A, B \leq G$ containing N and $\bar{A} = A/N$ and $\bar{B} = B/N$, then

1. $A \leq B$ if and only if $\bar{A} \leq \bar{B}$,
2. In this case, $[B : A] = [\bar{B} : \bar{A}]$,
3. $\overline{\langle A, B \rangle} = \langle \bar{A}, \bar{B} \rangle$,
4. $\overline{A \cap B} = \bar{A} \cap \bar{B}$,
5. $A \trianglelefteq G$ if and only if $\bar{A} \trianglelefteq G/N$.

Simple Groups and Normality

[1]**Definition 93:** A normal series for a group G is a finite sequence of subgroups G_0, G_1, \dots, G_n so that $\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_n = G$. (We mean only that $G_i \triangleleft G_{i+1}$, not in normal in G . We call $G_1/G_0, G_2/G_1, \dots, G_n/G_{n-1}$ the factors of the series provided they are nontrivial. The length of the series is the number of (nontrivial) factors. Given two series $1 \trianglelefteq H_0 \trianglelefteq H_1 \trianglelefteq \dots \trianglelefteq H_m = G$, (1), and $1 \trianglelefteq G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_n = G$, (2), we call (1) a refinement of (2) if $\{G_i : i = 0, 1, \dots, n\} \subseteq \{H_j : j = 0, 1, \dots, m\}$.

[1]**Example 94:**

1. (a) $Z_{60} \supseteq Z_{30} \supseteq Z_5 \supseteq 1$
- (b) $Z_{60} \supseteq Z_{30} \supseteq Z_{15} \supseteq Z_5 \supseteq 1$

The second series is a refinement of the first.

2. For any Z_n we can factor n to get the normal series for it.
3. $D_{2n} \supseteq \langle r \rangle \supseteq 1$

[2]**Definition 95:** We call a group G simple if its only normal subgroups are G and $\{1\}$. We call a normal series where each factor is simple a composition series.

[2]**Theorem 96:** (Jordan-Hölder Theorem) Every finite nontrivial group has a composition series and the factors are unique (up to order). That is if $G = N_n \supseteq N_{n-1} \supseteq \dots \supseteq N_0 = 1$ and $G = M_m \supseteq M_{m-1} \supseteq \dots \supseteq M_0 = 1$ are composition series then $m = n$ and here is some permutation, π of $\{1, 2, \dots, n\}$ such that

$$\frac{N_i}{N_{i-1}} \cong \frac{M_{\pi(i)}}{M_{\pi(i)-1}}, 1 \leq i \leq n.$$

[2]**Theorem 97:** (Feit-Thompson) If G is a simple group of odd order, then $G \cong Z_p$ for some prime p .

[1]**Definition 98:** A group G is solvable if it has a normal series with all factors abelian.

[1]**Proposition 99:** If $N \trianglelefteq G$, N , and G/N are solvable, then G is solvable.

[1]**Proposition 100:** If G is a finite abelian group and p is a prime dividing $|G|$, then there is an $x \in G$ with $|x| = p$.

Transpositions and the Alternating Group

[2]**Definition 101:** A transposition is a 2-cycle.

[1]**Lemma 102:**

1. Every n -cycle is a product of $n - 1$ transpositions $(a_1 a_2 \dots a_n) = (a_1 a_n)(a_1 a_{n-1})\dots(a_1 a_2)$.
2. Every element of S_n is a product of transpositions.
3. There are many ways to write elements as products of transpositions.
4. $(i j)^2 = 1$
5. $\langle (1 2), (2 3), \dots, (n - 1 n) \rangle = S_n$.

End of Exam 1 Material

[1]**Proposition 103:** Each $\sigma \in S_n$ can either only be written as a product of an even number of transpositions or only written as a product of an odd number of transpositions.

[1]**Definition 104:** Let $\Delta = \prod_{i,j=1}^n x_i - x_j$. Let $\sigma \in S_n$. Then we define the homomorphism $\epsilon : S_n \rightarrow (\{\pm 1, \cdot\})$ by requiring $\sigma(\Delta) = \epsilon(\sigma)\Delta$.

[1]**Proposition 105:** ϵ is onto. In fact, $\epsilon((i j)) = -1$.

[1]**Definition 106:** The alternating group on n elements, A_n , is the $\ker \epsilon$.

[1]**Lemma 107:**

1. $(a_1 a_2 \dots a_n) \in A_n$ if and only if m is odd.
2. $\sigma \in A_n$ if and only if it decomposes as a product of cycles with an even number of cycles of even length.
3. $|A_n| = \frac{n!}{2}$.
4. $A_n \trianglelefteq S_n$.

Applications of Group Actions

[1]**Lemma 108:** Notice that $g \in G$ is in the kernel of the action of a group G on A if and only if g is in the kernel of the homomorphism $g \mapsto \sigma_g$.

[2]**Definition 109:** We call the action faithful if the kernel is the identity.

[1]**Lemma 110:** For every group action from $G \times A$ to A , we have an associated faithful action from $G/(\text{kernel})$ to A . An action is faithful if and only if the associated homomorphism is injective.

[1]**Lemma 111:** Define the relation \sim on A by $a \sim b$ if and only if there exists $g \in G$ such that $g \cdot a = b$. This is an equivalence relation and the equivalence classes are orbits.

[1]**Definition 112:** We call an action transitive if it has only one orbit.

[1]**Example 113:**

1. S_n action on $\{1, \dots, n\}$. This is transitive as the whole set is the only orbit.
2. Let $A = \mathbb{Z} \times \mathbb{Z}$. Let $(\mathbb{Z}, +)$ act on A by $1 \cdot (x, y) = (x + 2, y + 1)$. Then $n \cdot (x, y) = (x + 2n, y + n)$. An orbit is the line of slope 1/2 intersected with the set A . This is not transitive. It is faithful though and $G_a = \{0\}$ for all $a \in A$.
3. Let $\mathbb{Z} \times \mathbb{Z}$ act on \mathbb{Z} by $(m, n) \cdot a = a + 2m + 10n$. The orbit of 1 is all odd integers, and the orbit of 0 is all even integers. Hence, the action is not transitive. The stabilizer of 1 is $\{(-5k, k) : k \in \mathbb{Z}\}$. Note that if we replace 10 by 3, then the $\gcd(2, 3) = 1$ and the action becomes transitive.

[1]**Theorem 114:** (Cosets and Orbits Theorem) Let G act on a set A with $a \in A$. There is a bijection between \mathcal{O}_a (orbit of a) and the left cosets of G_a in G given by $g \cdot a \mapsto gG_a$.

[1]**Corollary 115:**

1. $|\mathcal{O}_a| = |G : G_a|$
2. If G is finite, $|G| = |\mathcal{O}_a||G_a|$ for each a .
3. If $G_a = \{1\}$, then we have a bijection between G and \mathcal{O}_a .

[2]**Definition 116:** Let $H \leq G$. Define a left multiplication action $\text{go } G$ on the left cosets of H by $g \cdot (kH) \mapsto (gk)H$.

[1]**Definition 117:** If G is a group and $H \leq G$, then the coset action of G on H is the action of left multiplication by elements of G on the set of all cosets of H in G .

[2]**Theorem 118:** (Coset Action Theorem) For the coset action of G on $H \leq G$,

1. G acts transitively.
2. The stabilizer of the coset H is the elements in H .
3. The kernel of the action $\bigcap_{x \in G} xHx^{-1}$ which is the largest normal subgroup of G contained in H .

[2]**Theorem 119:** (Cayley's Theorem) Every group is isomorphic to a subgroup of some symmetric group. In particular, every finite group of order n is isomorphic to a subgroup of S_n .

[2]**Theorem 120:** If the order of the group G is n and p is the smallest prime dividing n , then any subgroup of index p is normal.

4 Graphs and Groups

[1]**Definition 121:** A graph is a triple (V, E, ϵ) . V is a set of vertices, E is a set of edges. If $V_2 = \{S \subseteq V : |S| = 2\}$, then $\epsilon : E \rightarrow V_2$. (See notes for examples.)

[1]**Definition 122:** A directed graph means each edge has a direction.

[1]**Definition 123:** A symmetry of a graph (V, E, ϵ) is a pair of bijections $\alpha_V : V \rightarrow V$ and $\alpha_E : E \rightarrow E$ such that for all $e \in E$ $\alpha_V(\epsilon(e)) = \epsilon(\alpha_E(e))$.

[1]**Definition 124:** The symmetry group of a graph is the set of symmetries with composition as the operation function, called $SYM(\text{graph})$. (See notes for examples.)

[1]**Lemma 125:** If e is the only edge between vertices v and w , then $\alpha_E(e)$ has to be the only edge between $\alpha_V(v)$ and $\alpha_V(w)$.

[1]**Definition 126:** We call $G \leq SYM((V, E, \epsilon))$ edge transitive if for all edges e and f , there is $(\alpha_E, \alpha_V) \in G$ with $\alpha_E(e) = f$, and vertex transitive if for all vertices v and w there is $(\alpha_E, \alpha_V) \in G$ with $\alpha_V(v) = w$. (See notes for examples.)

[1]**Theorem 127:** (Cayley's Better Theorem) If a group is finitely generated, then there is a locally finite connected directed graph Γ so that G is isomorphic to a subgroup of $SYM(\Gamma)$.

[1]**Definition 128:** (Cayley Graph of a Group G) The Cayley graph of a group G with a finite set of generators $S \subseteq G$. Vertices- are G . Think $V = \{v_g : g \in G\}$. Edges- for each $s \in S$, we draw $|G|$ many edges, one from each v_g to v_{gs} . (See notes for examples.)

5 Conjugation

[1]**Definition 129:** Let G act on itself by the action $g \cdot a = gag^{-1}$. This action is called conjugation. If $b = gag^{-1}$, then a and b are called conjugates. Conjugacy is an equivalence relation and the conjugacy class of an element is the set of all conjugates, i.e. the orbit under this action.

[1]**Lemma 130:**

1. $gag^{-1} = a$ if and only if $ga = ag$ if and only if $g \in C_G(a)$.
2. $\{1\}$ is always a conjugacy class.

3. $\{a\}$ is a conjugacy class if and only if $a \in Z(G)$.
4. If G is abelian, all conjugacy classes are singletons.
5. If $gag^{-1} = b$, then $ga^k g^{-1} = b^k$ for all $k \in \mathbb{Z}$ and all elements of the conjugacy class have the same order.

[1]**Lemma 131:** Let $\mathcal{P}(G)$ be the power set of G and define an action of G on $\mathcal{P}(G)$ by $g \cdot S = gSg^{-1} = \{gsg^{-1} : s \in S\}$. Then,

1. $|gSg^{-1}| = |S|$
2. This action is never transitive.

[1]**Proposition 132:** (Counting Conjugates) If G is a group and $S \subseteq G$, then the number of conjugates of S is $|G : N_G(S)|$. In particular, for $a \in G$, $N_G(a) = C_G(a)$ and the number of conjugates of a is $|G : C_G(a)|$.

[1]**Theorem 133:** (Class Equation) For a finite group G ,

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

where g_1, \dots, g_r are each chosen from a distinct conjugacy class with more than one element.

[1]**Theorem 134:** Let p be a prime and P be a group with order P^α for some $\alpha \geq 1$. Then $|Z(P)| > 1$.

[1]**Corollary 135:** If p is a prime and $|G| = p^2$, then G is isomorphic to either Z_{p^2} or $Z_p \times Z_p$. In particular, it is abelian.

[1]**Definition 136:** For $\sigma \in S_n$, the cycle type of σ is a list of positive integers n_1, n_2, \dots, n_r where

1. σ is a product of r disjoint cycles of lengths n_1, n_2, \dots, n_r .
2. $n_1 \leq n_2 \leq \dots \leq n_r$.

[1]**Lemma 137:**

1. If $(a_1 a_2 \cdots a_m)$ is an m -cycle in S_n and $\tau \in S_n$, then $\tau(a_1 a_2 \cdots a_m)\tau^{-1} = (\tau a_1 \tau a_2 \cdots \tau a_m)$.
2. The cycle type of σ is unique.
3. If σ and τ are conjugates in S_n , then they have the same cycle type.
4. If $(a_1 \cdots a_r)$ and $(b_1 \cdots b_r)$ are r -cycles in S_n , then any $\alpha \in S_n$ with $\alpha(a_i) = b_i, i = 1, \dots, r$, will satisfy $\alpha(a_1 \cdots a_r)\alpha^{-1} = (b_1 \cdots b_r)$.
5. If $\sigma, \tau \in S_n$ have the same cycle type, then they are conjugate.

[1]**Lemma 138:** If $H \trianglelefteq G$, then H is a union of conjugacy classes of G . That is, each conjugacy class of G is either in H or disjoint from H .

6 Automorphisms

[2]**Definition 139:** An automorphism of G is an isomorphism from G to itself. The set of automorphisms of G under the action of composition is a group denoted by $Aut(G)$.

[1]**Lemma 140:**

1. $Aut(G) \leq S(G)$.
2. For each $g \in G$ there is an automorphism given by $h \mapsto ghg^{-1}$. We call these inner automorphisms. These automorphisms form a subgroup of the automorphisms denoted by $Inn(G)$.
3. If G is abelian, the only inner automorphism is the identity.
4. $INN(G) \trianglelefteq AUT(G)$.

[2]**Proposition 141:** Let $H \trianglelefteq G$. Then G acts on H by $g \cdot h = ghg^{-1}$. Further the kernel of this action is $C_G(H)$, and $G/C_G(H)$ is isomorphic to a subgroup of $Aut(H)$.

[1]**Corollary 142:**

1. If $K \leq G$ and $g \in G$, then K and gKg^{-1} are isomorphic.
2. If $H \leq G$. Then $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $Aut(H)$.
3. $G/Z(G) \cong Inn(G) \leq Aut(G)$

[2]**Definition 143:** We say a subgroup K of G is characteristic, denoted $K \text{ char } G$ if $\alpha(K) = K$ for all $\alpha \in Aut(G)$.

[1]**Lemma 144:**

1. Characteristic implies normal.
2. $H \text{ char } K$ and $K \text{ char } G$ implies $H \text{ char } G$.
3. If $H \text{ char } K$ and $K \trianglelefteq G$, then $H \trianglelefteq G$.
4. Note that $H \trianglelefteq K$ and $K \text{ char } G$, does NOT imply $H \trianglelefteq G$.
5. $Z(G) \text{ char } G$.
6. If K is the unique subgroup of order $|K|$, then $K \text{ char } G$.
7. All subgroups of cyclic groups are characteristic.

[2]**Proposition 145:** If $|G| = pq$ with $p < q$ and p and q prime, then G is cyclic or p divides $q - 1$.

Sylow's Theorem

[1]**Definition 146:** Let G be a group and p be prime. Call any group H a p -group if $|H| = p^\alpha$ for some $\alpha \in \mathbb{N}$. If $H \leq G$, then we call it a p -subgroup of G . If $|G| = p^\alpha m$ with $(p, m) = 1$, then a subgroup of G of order p^α is called a Sylow p -subgroup of G . We use $Syl_p(G)$ for the set of all Sylow p -subgroups and $n_p = |Syl_p(G)|$.

[2]**Theorem 147:** (Sylow's Theorem) Let G be a finite group and p is a prime dividing $|G|$.

1. G has Sylow p -subgroups.
2. Any p -subgroup of G is conjugate to a subgroup of each Sylow p -subgroup. In particular, all Sylow p -subgroups are conjugate.
3. $|Syl_p(G)| \equiv 1 \pmod p$

[1]**Lemma 148:** If $P \in Syl_p(G)$, and Q is a p -subgroup, then $Q \cap N_G(P) = Q \cap P$.

[2]**Corollary 149:** For a Sylow p -subgroup P of a finite group G , TFAE:

1. P is unique; i.e. $n_p = 1$.
2. P is normal.
3. If $X \subseteq G$ such that for all $x \in X$, $|x|$ is a power of p , then $\langle X \rangle$ is a p -subgroup.

[1]**Remark:** If A and B are distinct subgroups of G of order p a prime, then $A \cap B = \{1\}$. As A and B are isomorphic to Z_p , every nonidentity element generates all of A or B . So if $A \cap B$ contains a nonidentity element, then $A = B$.

Direct Products

[1]**Definition 150:** Given the groups G_1, \dots, G_n , we define $G := G_1 \times G_2 \times \dots \times G_n$ to have elements (g_1, g_2, \dots, g_n) with each $g_i \in G_i$ for all $1 \leq i \leq n$ and operations $(g_1, g_2, \dots, g_n)(h_1, h_2, \dots, h_n) = (g_1h_1, g_2h_2, \dots, g_nh_n)$.

[1]**Lemma 151:**

1. G is a group.
2. $|G| = |G_1||G_2| \cdots |G_n|$.
3. For each i from 1 to n , the map from $I : G_i \rightarrow G$ given by $g \mapsto (1, 1, 1, \dots, g, \dots, 1, 1)$ where g is in the i^{th} -coordinate is an injective homomorphism.
4. For each i , the map $\pi_i : G \rightarrow G_i$ given by $(g_1, g_2, \dots, g_n) \mapsto g_i$ is a surjective homomorphism.
5. If $x \in I_i(G_i)$ and $y \in I_j(G_j)$ with $i \neq j$, then $xy = yx$.
6. Note that $I_i(G_i) \trianglelefteq G$ for each i and $G/I_i(G_i) \cong G_1 \times G_2 \times \dots \times G_{i-1} \times G_{i+1} \times \dots \times G_n$.
7. Also, $\ker \pi_i \cong G_1 \times G_2 \times \dots \times G_{i-1} \times G_{i+1} \times \dots \times G_n$.
8. If $x_i \in I_i(G_i)$ for $i = 1, \dots, n$, then $(x_1, x_2, \dots, x_n)^k = (x_1^k, x_2^k, \dots, x_n^k)$ for all $k \in \mathbb{Z}$. In particular, $|x_1 \cdots x_n| = \text{lcm}(|x_1|, |x_2|, \dots, |x_n|)$.
9. $Z(G) = Z(G_1) \times Z(G_2) \times \dots \times Z(G_n)$.

[1]**Definition 152:** Let G_λ for $\lambda \in \Lambda$ be a collection of groups. We define the direct product $\prod_{\lambda \in \Lambda} G_\lambda$ to be functions

$f : \Lambda \rightarrow \bigcup_{\lambda \in \Lambda} G_\lambda$ so that $f(\lambda) \in G_\lambda$. Given two such functions f and g , we define their product to be the function $h := fg$ given as follows $h(\lambda) = f(\lambda)g(\lambda)$.

[1]**Lemma 153:**

1. This is a group.
2. For each $\lambda \in \Lambda$, we have the function $\pi_\lambda : \prod_{\mu \in \Lambda} G_\mu \rightarrow G_\lambda$ given by evaluation at λ .
3. For each λ , we have a function, $I_\lambda : G_\lambda \rightarrow \prod_{\mu \in \Lambda} G_\mu$ given by sending $g \in G_\lambda$ to the function

$$h(\mu) := \begin{cases} g, & \text{if } \mu = \lambda, \\ 1_{G_\mu}, & \text{if } \mu \neq \lambda. \end{cases}$$

4. All of the properties from the list of properties above for finite products holds.

7 Extensions of Groups

[1]**Definition 154:** Given two groups N and Q , we call G an extension of N by Q if

1. $N \trianglelefteq G$,
2. $G/N \cong Q$.

[1]**Remark:** So we have an injective map $i : N \rightarrow G$ and a surjective map $\pi : G \rightarrow Q$ with $\text{im}(i) = \ker(\pi)$,

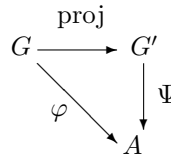
$$N \xrightarrow{i} G \xrightarrow{\pi} Q.$$

[1]**Definition 155:** For $x, y \in G$, let $[x, y] := x^{-1}y^{-1}xy$. We define the commutator subgroup of G to be $G' := \langle [x, y] : x, y \in G \rangle$. Note that often G' is strictly larger than $\{[x, y] : x, y \in G\}$.

[1]**Lemma 156:**

1. $xy = yx[x, y]$.

2. $xy = yx$ if and only if $[x, y] = 1$.
3. For $\sigma \in \text{Aut}(G)$, $\sigma([x, y]) = [\sigma(x), \sigma(y)]$. In particular, $[x, y]^{-1} = [x^{-1}, y^{-1}]$.
4. G' char G .
5. G/G' is abelian.
6. For all $H \trianglelefteq G$, G/H is abelian if and only if $G' \trianglelefteq H$.
7. For all abelian groups A and all homomorphisms $\varphi : G \rightarrow A$, $G' \leq \ker \varphi$ and there is a unique $\Psi : G/G' \rightarrow A$ so that the diagram below commutes:



- [1]**Definition 157:** The derived series of G is the sequence of groups $G = G^{(0)} \supseteq G^{(1)} \supseteq G^{(2)} \dots$ where $G^{(1)} = G'$, $G^{(2)} = [G', G']$, and so on. Observe that $G^{(i+1)}$ char G^i and $G^{(i)}/G^{(i+1)}$ is abelian for all i .
- [1]**Theorem 158:** For a finite group G , G is abelian if and only if $G^{(n)} = 1$ for some $n \geq 0$.
- [1]**Lemma 159:** If G is solvable, then the derived series is the shortest normal series of G with abelian factors.
- [1]**Definition 160:** The least positive integer n so that $G^{(n)} = 1$ is called the solvable length of G .
- [1]**Proposition 161:** An extensions of a solvable group by a solvable group is solvable, and the solvable length of the extensions is at most the sum of the two solvable lengths.
- [1]**Proposition 162:** (Counting Products) If $H, K \leq G$, then the number of ways of writing an element HK as a product of an elements of H and an element of K is $|H \cap K|$.
- [1]**Theorem 163:** (Recognition Theorem for Direct Products) If $H, K \leq G$ with $H \cap K = 1$, then $HK \cong H \times K$.
- [1]**Definition 164:** We call $H \times K$ an external direct product of H and K and HK an internal direct product of H and K .

8 Semi-direct Products

[1]**Theorem 165:** Let H and K be groups, $\varphi : K \rightarrow \text{Aut}(H)$ a homomorphism. We use $H \rtimes_{\varphi} K$ for the set of ordered pairs (h, k) , $h \in H$, and $k \in K$ with the operation $(h_1, k_1)(h_2, k_2) = (h_1\varphi_{k_1}(h_2), k_1k_2)$. Then $H \rtimes_{\varphi} K$ is a group and the following hold:

1. The map $h \mapsto (h, 1)$ is a homomorphism and $\{(h, 1) : h \in H\}$ is a normal subgroup.
2. The map $k \mapsto (1, k)$ is a homomorphism and $\{(1, k) : k \in K\}$ is a subgroup.
3. The intersection of the two subgroups is $(1, 1)$.

[1]**Theorem 166:** In this setting, the following are equivalent:

1. $H \rtimes_{\varphi} K$ is $H \times K$.
2. $\{(1, k) : k \in K\}$ is normal.
3. $\varphi_k = 1_H$ for all $k \in K$.

[1]**Theorem 167:** (Recognition Theorem for Semidirect Products) If $H, K \leq G$ with $H \trianglelefteq G$ and $H \cap K = 1$, then $HK \cong H \rtimes_{\varphi} K$ where $\varphi_k(h) = khk^{-1}$.

Ring Theory

[2]**Definition 168:** A ring is a set R with two operations $+$ and \cdot satisfying:

- (a) $(\mathbb{R}, +)$ is an abelian group.
- (b) \cdot is associative.
- (c) \cdot is distributive over $+$.

A unit in R is an element with a multiplicative inverse. We call a ring in which every nonzero element is a unit a division ring. A division ring in which \cdot is also commutative is called a field.

[1]**Example 169:**

1. $(\mathbb{Q}, +, \cdot)$ is a field.
2. Let X be a nonempty set. Let $F(X) := \{f : X \rightarrow \mathbb{C}\}$ and $+$ and \cdot be defined point-wise on elements of $F(X)$. Then $(F(X), +, \cdot)$ is a ring, but $(F(X), \cdot)$ is not a group. An element $f \in F(X)$ is a unit if and only if $0 \notin \text{Range}(f)$.

[1]**Definition 170:**

- (a) We call $x \in R$ a zero divisor if $x \neq 0$ and there exists $y \neq 0$ so that $xy = 0$.
- (b) Assume R has an identity $1 \neq 0$. An element u of R is called a unit in R if there is some v in R such that $uv = vu = 1$. The set of units in R is denoted by R^\times .

[1]**Definition 171:** We call a ring an integral domain if it has no zero divisors.

[1]**Proposition 172:** In an integral domain, if $a \cdot b = 0$, then $a = 0$ or $b = 0$.

[1]**Definition 173:** S is a subring of R if $S \subseteq R$, the ring operations of S agree with the ring operations of R , and S is closed under those operations.

[1]**Example 174:**

1. We use $C(X) = \{f \in F(X) : f \text{ is continuous.}\}$ This is a subring of $F(X)$. Note that $f(x) = x - \frac{1}{2}$ is not a zero divisor in $C([0, 1])$.
2. \mathbb{Z} is a subring of \mathbb{Q} .
3. $2\mathbb{Z} = \{2n : n \in \mathbb{Z}\}$ is a subring of \mathbb{Z} . There is no multiplicative identity in $2\mathbb{Z}$.
4. Let X be a metric space, i.e. \mathbb{R} . Define $C_c(X)$ to be functions f in $C(X)$ so that $\text{supp } f = \{x \in X : f(x) \neq 0\}$ is compact. This ring does not have an identity.

8.1 Quadratic (Integer) Rings

[1]**Definition 175:** Pick $D \in \mathbb{Z}$ square free, i.e. if n^2 divides D , then $n = 1$. Then we can define a subfield $\mathbb{Q}(\sqrt{D}) := \{a + b\sqrt{D} : a, b \in \mathbb{Q}\}$ of \mathbb{R} with the following operations:

- (a) $(a + b\sqrt{D}) + (c + e\sqrt{D}) = (a + c) + (b + e)\sqrt{D}$
- (b) $(a + b\sqrt{D})(c + e\sqrt{D}) = (ac + beD) + (ae + bc)\sqrt{D}$

The inverse of $a + b\sqrt{D}$ is $\frac{a-b\sqrt{D}}{a^2-Db^2}$ $\mathbb{Z}(\sqrt{D}) := \{a + b\sqrt{D} : a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{Q}(\sqrt{D})$. If $D \equiv 1 \pmod{4}$, then we can similarly define the subring $\mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right]$ of $\mathbb{Z}(\sqrt{D})$. For a square-free $D \in \mathbb{Z}$, we define

$$\mathcal{O}_D := \begin{cases} \mathbb{Z}[\sqrt{D}], & \text{if } D \equiv 2, 3 \pmod{4} \\ \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right], & \text{if } D \equiv 1 \pmod{4}. \end{cases}$$

We use ω for \sqrt{D} or $\frac{1+\sqrt{D}}{2}$ as appropriate from here on out. Note \mathcal{O}_{-1} is the Gaussian Integers.

[1]**Definition 176:** The field norm $N : \mathbb{Q}(\sqrt{D}) \rightarrow \mathbb{Q}$ is given by $N(a + b\sqrt{D}) = a^2 - Db^2$.

[1]**Lemma 177:**

1. $N(\pm 1) = 1$
2. $N(\alpha\beta) = N(\alpha)N(\beta)$ for $\alpha, \beta \in \mathbb{Q}(\sqrt{D})$.
3. If $\alpha \in \mathcal{O}_D$, $\alpha = a + b\omega$, then

$$M(\alpha) = \begin{cases} a^2 - Db^2, & \text{if } D \equiv 2, 3 \pmod{4}, \\ a^2 + ab + \frac{1-D}{4}b^2, & \text{if } D \equiv 1 \pmod{4}. \end{cases}$$

4. If $\alpha \in \mathcal{O}$, $N(\alpha) \in \mathbb{Z}$.
5. If α is a unit in \mathcal{O}_D , then $N(\alpha) = \pm 1$.

Polynomial Rings (Modules)

[1]**Definition 178:** Let R be a commutative ring. The polynomial ring $R[x]$ is the set $\{a_n x^n + \dots + a_1 x + a_0 : a_i \in R \text{ for all } 1 \leq i \leq n\}$ with the following operations:

- (a) Addition is performed component-wise.
- (b) Multiplications is defined by $ax^i \cdot bx^j = abx^{i+j}$ and then extended to all elements of $R[x]$ by the distributive property of the multiplication over addition.

Note that $R[x]$ is a commutative ring.

[2]**Proposition 179:** Let R be an integral domain. If $p, q \in R[x]$ with $p \neq 0$ and $q \neq 0$, then

1. $\deg(pq) = \deg(p) + \deg(q)$.
2. The units of $R[x]$ are the units of R .
3. $R[x]$ is an integral domain.

R is a subring of $R[x]$.

Matrix Rings

Let R be a ring and $n \geq 1$ be an integer.

[1]**Definition 180:** A matrix ring over R is the set $M_n(R)$ of all $n \times n$ matrices with entries in R . Addition is defined component-wise and multiplication is given by the usual matrix multiplication;

$$(a_{k\ell})(b_{kj}) = \sum_{k=1}^n a_{ik}b_{kj}.$$

Even if R is commutative, $M_n(R)$ is not commutative unless R is the trivial ring or $n = 1$.

Group Rings

[1]**Definition 181:** For a ring R and a group G , we define the group ring RG to be the set of all finite sums of elements of the form $r_i g_i$ with $r_i \in R$ and $g_i \in G$ with the following operations:

1. $r_i g_i + r_j g_j = (r_i + r_j)g_i g_j$,
2. $(r_i g_i)(r_j g_j) = r_i r_j (g_i g_j)$.

Note that the multiplication defined above can be extended using the distributive law of multiplication over addition.

[1]**Proposition 182:** R is a subring of RG . If G is finite, RG always has zero divisors.

Ring Homomorphisms, Quotients, and Ideals

[1]**Definition 183:** For rings R and S , $\varphi : R \rightarrow S$ is a ring homomorphism if

1. $\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2)$ for all $r_1, r_2 \in R$,
2. $\varphi(r_1 r_2) = \varphi(r_1)\varphi(r_2)$ for all $r_1, r_2 \in R$.

As usual, $\ker \varphi = \{r \in R : \varphi(r) = 0\}$. A bijective homomorphism is an isomorphism. Again, $\ker \varphi = \{0\}$ if and only if φ is 1-1.

[1]**Definition 184:**

1. Define $\varphi : R[x] \rightarrow R$ by $\varphi(p) = p(0)$. This is a ring homomorphism and $\ker \varphi$ is all polynomials with zero constant terms.
2. $\Psi : \mathbb{Z} \rightarrow n\mathbb{Z}$ given by $x \mapsto nx$ for some fixed $n \in \mathbb{Z}$ is **not** a ring homomorphism.
3. We can define the determinant map from $M_n(R)$ to R and this is a ring homomorphism. In fact,

$$\det((a_{ij})) = \sum_{\sigma \in S_n} \epsilon(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)}.$$

[1]**Definition 185:** We call $I \subseteq R$ a two-sided ideal if

1. For all $a, b \in I$, $a + b \in I$ (or $(I, +)$ is a subring of $(R, +)$).
2. For all $z \in I$ and $r \in R$, $ar, ra \in I$, or $rI, Ir \subseteq I$ for all $r \in R$.

[1]**Definition 186:** For a ring R and an ideal I , R/I is the set of cosets $r + I = \{r + i : i \in I\}$ for all $r \in R$ with operations

1. $(r + I) + (s + I) = (r + s) + I$,
2. $(r + I)(s + I) = rs + I$,

for all $r, s \in R$.

[1]**Proposition 187:** With these operations, R/I is a ring.

[1]**Proposition 188:** For any set $I \subseteq R$, the above definitions make R/I into a ring if and only if I is a two-sided ideal.

8.2 Isomorphism Theorems

[1]**Theorem 189:** (First Isomorphism Theorem)

1. If $\varphi : R \rightarrow S$ is a homomorphism of rings, then the kernel of φ is an ideal of R , the image of φ is a subring of S , and $R/\ker \varphi \cong \varphi(R)$.
2. If I is an ideal of a ring R , then the map $\pi : R \rightarrow R/I$ given by $\pi(r) = r + I$ is an onto ring homomorphism with $\ker \pi = I$.

[1]**Example 190:**

1. In $\mathbb{Z}[x]$, let I be all polynomials of degree 2 or more, or zero. Then I is **not** an ideal as $5x^2 + 6, 5x^2 \in I$ but their difference is not.
2. Let J be the polynomials with zero constant term and zero degree 1 coefficient. J is closed under addition. Define $\varphi : \mathbb{Z}[x] \rightarrow \mathbb{Z} \times \mathbb{Z}$ by $\varphi(p) = (p(0), p'(0))$. Then φ is a ring homomorphism and $\ker \varphi$ is J .
3. For $F([0, 1])$ and $x \in [0, 1]$, define $\varphi_x : F([0, 1]) \rightarrow \mathbb{C}$ by $\varphi_x(f) = f(x)$. Then $F([0, 1])/\ker \varphi_x \cong \mathbb{C}$.
4. Pick a ring R , an ideal J of R and $n \in \mathbb{N}$. Define a map $\pi^{(n)} : M_n(R) \rightarrow M_n(R/J)$ by sending $(r_{ij}) \mapsto (\pi(r_{ij}))$. Then $\ker \pi^{(n)} = M_n(J)$ and $M_n(J)$ is an ideal of $M_n(R)$.

[1]**Theorem 191:** (Second Isomorphism Theorem) If A is a subring of R and B is an ideal of R , then $A \cap B$ is an ideal of A and

$$\frac{A+B}{B} \cong \frac{A}{A \cap B}.$$

[1]**Theorem 192:** (Third Isomorphism Theorem) If I and J are ideals of R with $I \subseteq J$, then J/I is an ideal of R/I and

$$\frac{R/I}{J/I} \cong R/J.$$

[1]**Theorem 193:** (Fourth Isomorphism Theorem) If I is an ideal of R , the map from subrings of R containing I to subrings of R/I given by $A \mapsto A/I$ is an inclusion-preserving bijection. Moreover, A is an ideal of R if and only if A/I is an ideal of R/I .

[1]**Definition 194:** If I and J are ideals of R , then $I + J := \{i + j : i \in I, j \in J\}$ and $IJ := \{i_1j_1 + i_2j_2 + \dots + i_nj_n : i_k \in I, j_j \in J\}$. For $n \geq 1$, we define $I^n = \underbrace{I \cdots I}_n$.

[1]**Lemma 195:**

1. $I + J$ is the smallest ideal containing I and J .
2. IJ is an ideal contained in $I \cap J$.
3. IJ can be properly contained in $I \cap J$.

8.3 Properties of Ideals

[1]**Lemma 196:** For R a ring, $A \subseteq R$, the set $RAR = \{\sum_{i=1}^n r_i a_i s_i : a_i \in A, r_i, s_i \in R\}$ is the smallest ideal containing

A . We can similarly define AR and RA . If R is commutative, then $RA = AR = RAR$.

[1]**Definition 197:** If an ideal $I = (A)$ for A a finite set, we say I is finitely generated. If $I = (\{a\})$, then I is said to be principal.

[1]**Example 198:**

1. If $a \in R$, then $(a) = R$ if and only if a is a unit.
2. $(0) = \{0\}$ is a principal ideal.
3. If $I \neq (0)$ is an ideal of \mathbb{Z} , then $I = n\mathbb{Z}$ where n is the least positive element of I .
4. $(2, x) = \{p \cdot 2 + q \cdot x : p, q \in \mathbb{Z}[x]\}$ is a non-principal ideal in $\mathbb{Z}[x]$.

[1]**Lemma 199:**

1. For R a commutative ring, R is a field if and only if only ideals are $0, R$.
2. If $\varphi : F \rightarrow R$ a ring homomorphism and F is a field, then either $\varphi = 0$ or φ is injective.
3. For a ring R , R is a division ring if and only if the only left and right ideals of R are 0 and R .

[1]**Lemma 200:** (Zorn's Lemma) If, in a nonempty partially ordered set, every chain has an upper bound, then the set has a maximal element.

[1]**Definition 201:**

1. A partially ordered set is a binary relation, \leq , on a set that is reflexive, antisymmetric, and transitive.
2. A chain is a subset that is totally ordered (all elements are comparable).
3. An upper bound for a subset S is an element in the larger set such that $u \geq s$ for all $s \in S$.

4. A maximal element for the big set is an element of that set so that $m \leq x$ implies $x = m$ for all x in the big set.

[1]**Example 202:**

1. A set of subsets of \mathbb{N} ordered by inclusion is a partially ordered set.
2. A set of open subsets of \mathbb{R} containing 0 ordered by reverse inclusion is a partially ordered set.
3. Pick $[a, b] \subseteq \mathbb{R}$ and order the set of partitions of $[a, b]$ by inclusion. This set is partially ordered.

[1]**Definition 203:** An ideal M in a ring R is maximal if $M \neq R$ and the only ideals of R containing M are M and R .

[1]**Proposition 204:** In a ring with identity, every proper ideal is contained in a maximal ideal.

[1]**Proposition 205:** Let R be a commutative ring and M an ideal of R , then M is maximal if and only if R/M is a field.

[1]**Definition 206:** In a commutative ring R , we call an ideal I a prime ideal if for any $a, b \in R$, $ab \in I$ implies $a \in I$ or $b \in I$.

[1]**Proposition 207:** Let R be a commutative ring and I an ideal, then I is prime if and only if R/I is an integral domain.

[1]**Corollary 208:** As every field is an integral domain, every maximal ideal is prime.

Math 818 Notes

[1]**Theorem 209:** Let R be a commutative ring and $D \subseteq R$ be a nonempty subset of $R \setminus \{0\}$ which is closed under multiplication and has no zero divisors. Then there is a commutative ring with identity, Q , and an injective ring homomorphism $i : R \rightarrow Q$ so that

- (0) For all $d \in D$, $i(d)$ is a unit.
- (1) For all $q \in Q$ there are $r \in R$ and $d \in D$ such that $q = i(r)i(d)^{-1}$.
- (2) If S is a commutative ring with identity and $\varphi : R \rightarrow S$ has for all $d \in D$, $\varphi(d)$ is a unit, then there is $\Phi : Q \rightarrow S$ so that $\varphi = \Phi \circ i$. If φ is one-to-one, then Φ can be chosen to be one-to-one.

[1]**Definition 210:** If F is a field and $A \subseteq F$, then the subfield of F generated by A is the intersection of all the subfields of F containing A . Note this intersection really is a subfield.

[1]**Corollary 211:** Let R be an integral domain with $R \subseteq Q$, its field of fractions. For any field F containing a subring R' isomorphic to R , the subfield of F generated by R' is isomorphic to Q .

[1]**Example 212:**

1. The field of fractions of a field F is F .
2. The field of fractions of \mathbb{Z} is \mathbb{Q} .
3. The field of fractions of $2\mathbb{Z}$ is \mathbb{Q} .
4. The field of fractions of \mathcal{O}_D is $\mathbb{Q}(\sqrt{D})$.
5. For an integral domain R , the field of rational functions is $\frac{p(x)}{q(x)}$ where $p(x), q(x) \in R[x]$ and $q(x) \neq 0$ is the field of fractions of $R[x]$. It contains the field of fractions of R , and if R happens to be a field, it is denoted by $R(x)$. In fact, if $r = \frac{p(x)}{q(x)}$ with $p, q \in \mathbb{Q}[x]$, let N be the least common multiple of the denominator of the coefficients of p and q . So $np, Nq \in \mathbb{Z}[x]$ and $\frac{p}{q} = \frac{Np}{Nq}$. So the field of fraction for $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$ are both $\mathbb{Q}(x)$.

Factorizations in Rings

8.4 Euclidean Domain

[1]**Definition 213:** A norm on an integral domain R is a function $N : R \rightarrow (\mathbb{Z}^+ \cup \{0\})$ such that $N(0) = 0$. If 0 is the only element such that $N(0) = 0$, then the norm is called positive.

[1]**Definition 214:** We call R a Euclidean domain if there is a norm N on R such that for all $a, b \in R$ with $b \neq 0$, there are $q, r \in R$ such that $a = qb + r$ and $r = 0$ or $N(r) < N(b)$.

[1]**Definition 215:**

1. In a field F , we can pick any norm. In particular, $N(x) = 0$ for all $x \in F$. For $a, b \in F$, $b \neq 0$ we have $a = qb + 0$ with $q = ab^{-1}$.
2. In \mathbb{Z} , we can use $N(a) = |a|$. We warn that $q, r \in R$ are not unique though.
3. For a field F , $F[x]$ is a Euclidean domain with norm $N(p(x))$ is the degree of p .
4. Recall \mathcal{O}_D inside $\mathbb{Q}(\sqrt{D})$. We have a norm on \mathcal{O}_D given by $N(a + b\sqrt{D}) = |a^2 - Db^2|$ for $D \not\equiv 1 \pmod{4}$.

[1]**Proposition 216:** A Euclidean domain is principal, i.e. every ideal I has an element d of the domain with $I = (d)$.

[1]**Corollary 217:** If an integral domain has a non principal ideal, then it is not an Euclidean domain.

[1]**Example 218:**

1. \mathbb{Z} is a principal ideal domain (PID).
2. $\mathbb{Z}[\sqrt{-5}]$ is no Euclidean.

[1]**Definition 219:** Let R be a commutative ring and $a, b \in R$ with $b \neq 0$. The element a is a multiple of b or b is a divisor of a if $a = rb$ for $r \in R$. A greatest common divisor of $a, b \in R$ is $d \in R$ with $d \neq 0$ so that

- (i) $d|a$ and $d|b$
- (ii) If $e|a$ and $e|b$, then $e|d$.

We use (a, b) or $\gcd(a, b)$ to represent the greatest common divisor.

[1]**Lemma 220:**

1. If $b|a$ and u is a unit, then $ub|a$.
2. $a|b$ if and only if $b \in (a)$ if and only if $(b) \subseteq (a)$.
3. $d|b$ and $d|a$ if and only if $a, b \in (d)$ if and only if the ideal generated by a and b , (a, b) , satisfies $(a, b) \subseteq (d)$.

[1]**Proposition 221:** If the ideal (a, b) is such that $(a, b) = (d)$, then d is a greatest common divisor of a and b . The converse is false.

[1]**Proposition 222:** In an integral domain R , if $d, d' \in R$ and $(d) = (d')$, then there is a unit u in R with $d = ud'$.

[1]**Proposition 223:** If d and d' are both greatest common divisors of a and b , then there is a unit u in R with $d = ud'$.

[1]**Example 224:** (Euclidean Algorithm) Given a, b in a Euclidean domain R , with $a, b \neq 0$. We define sequences r_0, r_1, \dots, r_n and q_0, q_1, \dots, q_{n+1} by

$$\begin{aligned} a &= q_0b + r_0 \\ b &= q_1r_0 + r_1 \\ &\vdots \\ &\vdots \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} r_n. \end{aligned}$$

We know that $N(b) > N(r_0) > N(r_1) > \dots > N(r_n)$. Since this is bounded below, there is some $n \in \mathbb{N}$ such that $r_{n-1} = q_{n+1}r_n$.

[1]**Theorem 225:**

1. r_n is a gcd of a and b in the above setting.
2. There exists $x, y \in R$ such that $r_n = ax + by$.

[1] **Example 226:** $\mathbb{Z} \left[\frac{1+\sqrt{-19}}{2} \right]$ is not Euclidean but is a P.I.D.

[2] **Definition 227:** Let R be an integral domain and $\tilde{R} = \{0\} \times R^\times$. We call $u \in R \setminus \tilde{R}$ a universal side divisor (USD) if for all $x \in R$, there is $q \in R$ and $z \in \tilde{R}$ such that $x = qu + z$.

[2] **Proposition 228:** A Euclidean domain which is not a field has universal side divisors.

[2] **Proposition 229:**

1. If R is a P.I.D. with $a, b \in R$, with neither zero, then $\gcd(a, b)$ exists and is unique.
2. Moreover, there are $x, y \in R$ such that $\gcd(a, b) = ax + by$.

[1] **Corollary 230:** For any commutative ring R , $R[x]$ is a P.I.D. if and only if R is a field.

[1] **Proposition 231:** In a P.I.D., prime ideals are maximal.

[1] **Definition 232:** A norm N in a commutative ring R is a Dedekind-Hasse (DH) norm if it is positive and for all $a, b \in R \setminus \{0\}$, either $a \in (b)$ or there are $s, t \in R$ such that $N(sa - tb) < N(b)$.

[1] **Proposition 233:** An integral domain is a P.I.D. if and only if it has a (DH) norm.

8.5 Unique Factorization Domain

[1] **Definition 234:** In an integral domain R , we say $a, b \in R$ are associate if $a = ub$ for some unit $u \in R$. This is an equivalence relation.

[1] **Definition 235:** In an integral domain R , we call $p \in R$ prime if $p|ab$ then $p|a$ or $p|b$. We call $r \in R$ irreducible if $r \neq 0$, r is not a unit, and whenever $r = ab$ for $a, b \in R$, then at least one of a or b is a unit. Otherwise, r is reducible.

[1] **Proposition 236:** In an integral domain, every prime element is irreducible.

[1] **Example 237:** In $\mathbb{Z}[\sqrt{-5}]$, 3 is irreducible, but not prime.

[1] **Proposition 238:** In a P.I.D., an irreducible element is prime.

[1] **Definition 239:** We call an integral domain R a unique factorization domain (UFD) if for all $r \in R$, r not zero or a unit, we have

1. r can be written as a finite product of irreducibles, i.e. $r = p_1 p_2 \cdots p_n$.
2. If $r = q_1 \cdots q_m$ for irreducibles q_1, q_2, \dots, q_m , then $m = n$ and there is $\pi \in S_n$ so that $q_{\pi(i)}$ and p_i are associates.

[1] **Example 240:**

1. If F is a field, F is a UFD.
2. \mathbb{Z} is a UFD, and so $\mathbb{Z}[x]$ is a UFD.
3. $F[x]$ for a field F is a UFD.
4. $\mathbb{Z}[2i]$ is not a UFD.
5. $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

[1] **Proposition 241:** In a UFD, a (nonzero) element is prime if and only if it is irreducible.

[1] **Definition 242:** We call a commutative ring R Noetherian if, whenever we have a sequence of ideals of R , $I_1 \subset I_2 \subset \dots$, then there is some $n \in \mathbb{N}$ such that for all $m \geq n$, $I_m = I_n$.

[1] **Theorem 243:** Every PID is Noetherian.

[1] **Theorem 244:** Every PID is a UFD.

[1] **Corollary 245:** \mathbb{Z} is a UFD.

[1] **Corollary 246:** If R is a PID, then there is a multiplicative DH norm on R .

8.6 Polynomial Rings

[1]**Definition 247:** Let $(\mathbb{Z}^n)_+ := \{(z_1, \dots, z_n) : z_i \in \mathbb{Z}, z_i \geq 0\}$ and define the polynomial ring in variables x_1, x_2, \dots, x_n with coefficients in R , $R[x_1, \dots, x_n]$, in the following way. Define the function $f : (\mathbb{Z}^n)_+ \rightarrow R$ which are zero at all but finitely many elements of $(\mathbb{Z}^n)_+$, where $ax_1^{d_1} \cdots x_n^{d_n}$ is represented by the function f satisfying $f(d_1, d_2, \dots, d_n) = a$. We define addition pointwise here and multiplication is given by

$$(f \cdot g)(d_1, d_2, \dots, d_n) = \sum_{\substack{e_i + h_i = d_i \\ i=1, \dots, n}} f(e_1, \dots, e_n)g(h_1, \dots, h_n).$$

[1]**Definition 248:** For a monomial $ax_1^{d_1} \cdots x_n^{d_n}$, we have:

1. Its degree is $d_1 + d_2 + \dots + d_n \in \mathbb{N} \cup \{0\}$.
2. Its multidegree is $(d_1, d_2, \dots, d_n) \in (\mathbb{N} \cup \{0\})^n$.
3. A polynomial is homogeneous of degree k if all its monomials have degree k .
4. Every polynomial can be written uniquely as the sum of homogeneous polynomials $p = f_0 + f_1 + \dots + f_d$, where each f_i is homogeneous of degree i .
5. We can define polynomials in variables x_1, x_2, \dots , by considering the ring $\cup_{n \geq 1} R[x_1, \dots, x_n]$. Using induction, we can show from the function definition that $(R[x_1, \dots, x_{n-1}])[x_n] \cong R[x_1, \dots, x_n]$.

[1]**Proposition 249:** Let R be an integral domain.

1. $R[x_1, \dots, x_n]$ is an integral domain.
2. The units of $R[x_1, \dots, x_n]$ are the units of R .
3. For $p, q \in R[x_1, \dots, x_n]$, not zero, $\deg(p + q) \leq \max\{\deg(p), \deg(q)\}$ and $\deg(pq) \leq \deg(p) + \deg(q)$.

[1]**Definition 250:** For an ideal I of a commutative ring R , the reduction homomorphism $\varphi : R[x] \rightarrow (R/I)[x]$,

sends a polynomial $\sum_{i=1}^n a_i x^i$ to $\sum_{i=1}^n (a_i + I)x^i$.

[1]**Lemma 251:**

1. φ is an onto ring homomorphism.
2. $\ker \varphi = I[x]$
3. $I[x]$ is the ideal of $R[x]$ generated by I , denoted (I) .
4. $R[x]/(I) \cong (R/I)[x]$
5. If I is prime, so is (I) .
6. I maximal $\not\Rightarrow (I)$ is maximal.

[1]**Theorem 252:** If F is a field, then $F[x]$ is a Euclidean Domain.

[1]**Corollary 226:** If F is a field, then $F[x]$ is a PID and UFD.

[1]**Example 227:**

1. $\mathbb{Z}[x]$ is not a PID, but $(\mathbb{Z}/p\mathbb{Z})[x]$ is a PID.
2. Since \mathbb{Q} is a field, $\mathbb{Q}[x]$ is a PID. Since \mathbb{Q} is not a field, $\mathbb{Q}[x, y]$ is not a PID.

[1]**Proposition 228:**

1. If $R[x]$ is a UFD, so is R .
2. $R[x]$ is a subring of $F[x]$.

3. Even if $p(x)$ is irreducible in $F[x]$, it might be reducible in $R[x]$.
4. If R is a UFD and $a \in R$ is irreducible, a is a prime in $R[x]$.

[2]**Theorem 229:** (Gauss's Lemma) Let R be a UFD with the field of fractions F . If $p(x) \in R[x]$ is reducible in $F[x]$, then $p(x)$ is irreducible in $R[x]$. Moreover, if $p(x) = A(x)B(x)$ for some $A(x), B(x) \in F[x]$, then there are $r, s \in F[x] \setminus \{0\}$ so that $rA(x), sB(x) \in R[x]$, and $p(x) = (rA(x))(sB(x))$.

[1]**Corollary 230:** (Primitive Corollary) Let R be a UFD with the field of fractions F . If a gcd of the coefficients of $p(x) \in R[x]$ is 1, then $p(x)$ is irreducible in $R[x]$ if and only if it is irreducible in $F[x]$.

[1]**Definition 231:** We say $p(x) \in R[x]$ is primitive if a gcd of the coefficients of $p(x)$ is a unit.

[1]**Theorem 232:** R is a UFD if and only if $R[x]$ is a UFD.

[1]**Corollary 233:** If R is a UFD, then so is $R[x_1, x_2, \dots, x_n]$ and $R[x_1, x_2, \dots]$.

Easy Tests for Irreducibility

[1]**Proposition 234:**

1. If $p(x) \in F[x]$, with F a field, then $p(x)$ has $x - \alpha$ as a factor if and only if $p(\alpha) = 0$.
2. If $p(x) \in F[x]$, with F a field and $\deg(p(x)) \leq 3$, then $p(x)$ is reducible if and only if p has a root.
3. (This is stated for \mathbb{Z} and \mathbb{Q} , but works for any UFD R and its field of fractions F) If $r/s \in \mathbb{Q}$ (in lowest terms) is a root of $a_n x^n + \dots + a_1 x + a_0$ in $\mathbb{Z}[x]$, then $r|a_0$ or $s|a_n$.
4. Roots of $x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0$ are divisors of a_0 .
5. If R is an integral domain, I is a proper ideal, and $p(x)$ is a nonconstant monic polynomial, then if $p(x) = a(x)b(x)$ in $R[x]$, then in $(R/I)[x]$, $\overline{p(x)} = \overline{a(x)}\overline{b(x)}$.
6. In the context of (5), if $\overline{p(x)} \in (R/I)[x]$ is irreducible, so is $p(x)$ in $R[x]$.

[2]**Theorem 235:** (Eisenstein's Criteria) Let R be an integral domain and P be a prime ideal. If $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0$ in $R[x]$ has a_{n-1}, \dots, a_0 all in P and $a_0 \notin P^2$, then $f(x)$ is irreducible in $R[x]$.

Modules

[1]**Definition 236:** Let R be a ring. We say V is a left R -module over a ring R if

- (i) $(V, +)$ is an abelian group.
- (ii) $\cdot : R \times V \rightarrow V$ is such that
 - (a) $(r + s) \cdot v = r \cdot v + s \cdot v$,
 - (b) $r \cdot (s \cdot v) = (rs) \cdot v$,
 - (c) $r \cdot (v_1 + v_2) = r \cdot v_1 + r \cdot v_2$,
 - (d) If R has an identity, $1 \cdot v = v$.

[1]**Example 237:**

1. A vector space over a field F is an F -module.
2. If R is a ring, then left $R^2 = \{(r, s) : r, s \in R\}$ with $(r, s) + (a, b) = (r + a, s + b)$ and $r \cdot (a, b) = (ra, rb)$. Then this is an R -module.
3. We call R^n the free R -module of rank n for $n = 1, 2, \dots$
4. Consider \mathbb{Z}_2 , the finite field. Define a scalar multiplication $\cdot : \mathbb{Z} \times \mathbb{Z}_2 \rightarrow \mathbb{Z}_2$ by $a \cdot \overline{b} := \overline{ab}$. Then \mathbb{Z}_2 is a \mathbb{Z} -module.

5. Let A be an abelian group. Define $\cdot : \mathbb{Z} \times A \rightarrow A$ by

$$n \cdot a = \begin{cases} a + a + \dots + a, & \text{if } n > 0, \\ 0, & \text{if } n = 0, \\ -a + -a + \dots + -a, & \text{if } n < 0. \end{cases}$$

Then, A is a \mathbb{Z} -module.

[1]**Proposition 238:** Every \mathbb{Z} module arises from an abelian group in exactly this way.

We now assume that all rings R are unital.

[2]**Definition 239:** Let R be a ring and let M be an R -module. An R -submodule of M is a subgroup of M which is closed under the action of ring elements, i.e. $rn \in N$ for all $r \in R, n \in N$.

[2]**Proposition 240:** (The Submodule Criterion) Let R be a ring and M be an R -module. A subset N of M is a submodule of M if and only if

1. $N \neq \emptyset$
2. $x + ry \in N$ for all $r \in R$ and for all $x, y \in N$.

[2]**Definition 241:** Let R be a commutative ring with identity. An R -algebra is a ring A with identity together with a ring homomorphism $f : R \rightarrow A$ mapping 1_R to 1_A such that the subring $f(R) \subseteq Z(A)$.

[1]**Proposition 242:** Let R be a unital commutative ring. Then A is an R -algebra if and only if A is an R -module with a multiplication $\times : A \times A \rightarrow A$ such that $r \cdot (a \times b) = (r \cdot a) \times b = a \times (r \cdot b)$ and $(A, +, \times)$ is a unital ring.

[2]**Definition 243:** If A and B are two R -algebras, an R -algebra homomorphism is a ring homomorphism $\varphi : A \rightarrow B$ mapping 1_A to 1_B such that $\varphi(r \cdot a) = r \cdot \varphi(a)$ for all $r \in R$ and $a \in A$.

Module Homomorphisms and Quotients

[1]**Definition 244:**

(a) If M, N are R -modules for some ring R , then we call $\varphi : M \rightarrow N$ an R -module homomorphism if

- (i) $\varphi(x + y) = \varphi(x) + \varphi(y)$ for all $x, y \in M$,
- (ii) $\varphi(rx) = r\varphi(x)$, for all $x \in M, r \in R$.

We use $\text{Hom}_R(M, N)$ for the set of these maps.

- (b) $\ker \varphi := \{x \in M : \varphi(x) = 0\}$.
- (c) $\text{Im}(\varphi) = \varphi(M) = \{y \in N : \text{There exists } x \in M \text{ such that } \varphi(x) = y\}$.
- (d) An R -module isomorphism is a bijective homomorphism.

[1]**Remark:**

- (a) Remember that ring homomorphisms and module homomorphisms do not always correspond to each other.
- (b) If R is a field, then the R -module homomorphisms are called linear transformations.
- (c) The canonical projection map from R^n to R is an R -module homomorphism.
- (d) \mathbb{Z} -module homomorphisms are the same as the abelian group homomorphisms.

[1]**Proposition 245:**

- (a) φ is an R -module homomorphism if and only if $\varphi(rx + y) = r\varphi(x) + \varphi(y)$ for all $r \in R$ and x, y in the R -module.
- (b) For all $\varphi, \Psi \in \text{Hom}_R(M, N)$, we define

- (i) $(\varphi + \Psi)(x) = \varphi(x) + \Psi(x)$,

(ii) $(r\varphi)(x) = r\varphi(x)$.

Then $\text{Hom}_R(M, N)$ is an R -module.

1. Let $\varphi \in \text{Hom}_R(M, N)$ and $\Psi \in \text{Hom}_R(N, L)$, then $\Psi \circ \varphi \in \text{Hom}_R(M, L)$.
2. Under the above operation, $\text{Hom}_R(M, M)$ is a ring with identity. So if R is commutative, $\text{Hom}_R(M, M)$ is an R -algebra.

[1]**Definition 246:** Let R be a ring, M an R -module, and N a submodule of M . Then the abelian quotient group M/N with the multiplication $\cdot : R \times M/N \rightarrow M/N$ given by $r \cdot (x + N) = rx + N$ is an R -module. Moreover, the map $\pi : M \rightarrow M/N$ with $x \mapsto x + N$ is an R -module homomorphism with $\ker \pi = N$.

Sums, Intersections, and Nested Unions of Modules

[1]**Definition 247:** If A and B are submodules of an R -module M , then $A + B := \{a + b : a \in A, b \in B\}$ is an R -submodule, in fact the smallest submodule, containing A and B .

[1]**Proposition 248:**

(a) If N_1, \dots, N_k are submodules, so is $\bigcap_{i=1}^k N_i$.

(b) If $N_1 \subseteq N_2 \subseteq \dots$ are submodules an R -module N , then so is $\bigcup_{i=1}^{\infty} N_i$.

[2]**Theorem 249:** (Module Isomorphism Theorems)

- (a) Let M and N be R -modules and let $\varphi : M \rightarrow N$ be an R -module homomorphism. Then $\ker \varphi$ is a submodule of M and $M/\ker \varphi \cong \varphi(M)$.
- (b) Let A and B be submodules of the R -module M . Then $(A + B)/B \cong A/(A \cap B)$.
- (c) Let M be an R -module, and let A and B be submodules of M with $A \subseteq B$. Then $(M/A)/(A/B) \cong M/B$.
- (d) Let N be a submodule of the R -module M . There is a bijection between the submodules of M which contain N and the submodules of M/N . The correspondence is given by $A \mapsto A/N$ for all $A \supseteq N$. This correspondence commutes with the processes of taking sums and intersections.

[1]**Definition 250:** Let M be an R -module and $A \subseteq M$, the submodule of M generated by A is $\bigcap \{N : N \text{ is a submodule of } M, A \subseteq N\}$. This is the smallest submodule of M containing A . It is denoted RA . If $|A| = 1$, then RA is called cyclic.

[1]**Proposition 251:** For $A \subseteq M$ with M and R -module,

$$RA = \{r_1 a_1 + \dots + r_n a_n : r_i \in R, a_i \in A\}.$$

[1]**Remark:** The submodules of ${}_R R$ are left modules, as they must be closed under addition and multiplication by elements of R .

[1]**Theorem 252:** (Structure Theorem for Cyclic Modules) Let R be a ring with identity and M a cyclic R -module. Then $M \cong_R (R/I)$ where I is some left ideal of R .

[1]**Corollary 253:** The Structure Theorem for Cyclic Groups follows from this.

[1]**Example 254:** Consider $M = \{(a, b) : a \in \mathbb{Z}, b \in \mathbb{Z}/10\mathbb{Z}\}$ as a \mathbb{Z} -module with $k(a, b) = (ka, kb)$. Let $x = (0, 1)$. Then $\mathbb{Z}x \cong \mathbb{Z}/10\mathbb{Z}$. Now $\text{ann } x = \{k \in \mathbb{Z} : k \cdot (0, 1) = (0, 0) \text{ in } M\}$, i.e. $10\mathbb{Z}$, and $\text{ann } (1, 0) = \{0\}$.

[1]**Definition 255:** Let $T : V \rightarrow V$ be a linear transformation. We have V as a $F[x]$ -module, given by $p(x)V = p(T)v$ for $v \in V$. A vector v is a cyclic vector if $\{v, Tv, T^2v, \dots\}$ spans V .

8.7 Direct Products and Direct Sums of Modules

[1]**Proposition 256:** Let M_1, M_2, \dots, M_k be R -modules. Take $M_1 \times M_2 \times \dots \times M_k = \{(m_1, \dots, m_k) : m_i \in M_i\}$ with componentwise addition and scalar multiplication give by $r(m_1, \dots, m_k) = (rm_1, \dots, rm_k)$. Thus us a left R -module written $M_1 \oplus M_2 \oplus \dots \oplus M_k$, and is called the direct sum of M_1, \dots, M_k .

[1]**Proposition 257:** (Internal Direct Sum Proposition) Let N_1, \dots, N_k be R -submodules of an R -module M . Define $\pi : N_1 \times \dots \times N_k \rightarrow N_1 + \dots + N_k$ by $\pi(n_1, \dots, n_k) = n_1 + \dots + n_k$. Then TFAE:

- (a) π is an isomorphism.
- (b) For $j = 1, \dots, k$,

$$N_j \cap (N_1 + \dots + N_{j-1} + N_{j+1} + \dots + N_k) = \{0\}.$$

- (c) Every $x \in N_1 + \dots + N_k$ can be written uniquely as $x = a_1 + \dots + a_k$ where $a_i \in N_i$.

[1]**Definition 258:** We say an R module F is free on a set $A \subseteq F$ if for all $x \in F \setminus \{0\}$, there are unique elements $r_1, \dots, r_n \in R \setminus \{0\}$ and $a_1, a_2, \dots, a_n \in A$ so that $x = a_1 r_1 + \dots + a_n r_n$. We call A a basis or set of free generators of F .

[1]**Theorem 259:** (Universal Property of Free Modules) For any set A and ring, R , with identity, there is a free R -module, $F(A)$, on the set A . Moreover, for any R -module N and function $\varphi : A \rightarrow N$, there is a unique R -module homomorphism $\Phi : F(A) \rightarrow N$ so that $\Phi(a) = \varphi(a)$ for all $a \in A$.

[1]**Corollary 260:**

- (1) If F_1 and F_2 are both free R -modules on a common set A , then there is a unique R -module isomorphism $\Psi : F_1 \rightarrow F_2$ so that $\Psi(a) = a$ for all $a \in A$.
- (2) If F is a free R -module on the set A , then F is isomorphic to $F(A)$.

9 Linear Algebra and Vector Spaces

[1]**Definition 261:** For a vector space V over a field F , we call $S \subseteq V$ a basis for V if

- (a) For all $s_1, \dots, s_n \in S, \alpha_1, \dots, \alpha_n \in F$, if $\alpha_1 s_1 + \dots + \alpha_n s_n = 0$, then $\alpha_1 = \dots = \alpha_n = 0$.
- (b) $\text{span } S = \{\alpha_1 s_1 + \dots + \alpha_n s_n : \alpha_i \in F, s_i \in S\}$.

[1]**Proposition 262:** Let $A = \{a_1, \dots, a_n\} \subset V$ with V a vector space. Then A is a basis if and only if A spans V and no proper subset of A spans V .

[1]**Corollary 263:** If a finite set spans a vector space, then the set contains a basis.

[1]**Lemma 264:** (Replacement Lemma) Suppose S and T are finite disjoint sets in a vector space V so that $S \cup T$ is a basis. If $x \notin \text{span } S$, then there is $t \in T$ such that $(S \cup \{x\}) \cup (T \setminus \{t\})$ is a basis.

[1]**Theorem 265:** (Replacement Theorem) Let A be a finite basis for a vector space V , and $b_1, \dots, b_m \in V$ be linearly independent. Then we can order A as a_1, \dots, a_n so that for $k = 1, \dots, \min\{m, n\}$, $\{b_1, \dots, b_k, a_{k+1}, \dots, a_n\}$ is a basis.

[1]**Corollary 266:** If a vector space V has a basis β with $|\beta| = n \in \mathbb{N}$, then

- (1) Every linearly independent set in V has at most n elements.
- (2) Every spanning set in V has at least n elements.
- (3) Every basis in V has exactly n elements.

[1]**Definition 267:** For a vector space V , $\text{dim } V$ is the cardinality of a basis.

[1]**Corollary 268:** Every linearly independent set can be enlarged to form a basis.

[1]**Theorem 269:** If a vector space V over some field F has $\text{dim } V = n \in \mathbb{N}$, then $V \cong F^n$.

[1]**Theorem 270:** Let V be a vector space over F and W be a subspace of V . Then $\text{dim } V = \text{dim } W + \text{dim } (V/W)$. If $\text{dim } V < \infty$, then $\text{dim } V - \text{dim } W = \text{dim } (V/W)$.

[1]**Corollary 271:** (Rank + Nullity Theorem) For $T : V \rightarrow W$ a linear transformation, $\text{dim } \ker T + \text{dim } T(V) = \text{dim } V$.

[1]**Corollary 272:** If $T : V \rightarrow W$ is a linear transformation and $\text{dim } V = \text{dim } W < \infty$, then TFAE:

- (1) T is an isomorphism.
- (2) $T(V) = W$.
- (3) $\ker T = \{0\}$.
- (4) T maps a basis of V to a basis of W .

9.1 Matrix of a Linear Transformation

[1]**Definition 273:** Given $T \in \text{Hom}(V, W)$ and the bases $\beta = (b_1, \dots, b_n) \subset V$ and $\xi = (e_1, \dots, e_m) \subset W$, the matrix of T with respect to β and ξ is

$$M_{\beta}^{\xi}(T) = \begin{pmatrix} \alpha_{1,1} & \cdots & \alpha_{1,n} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \alpha_{m,1} & \cdots & \alpha_{m,n} \end{pmatrix},$$

where

$$\begin{aligned} T(b_1) &= \alpha_{1,1}e_1 + \dots + \alpha_{m,1}e_m, \\ &\cdot \\ &\cdot \\ &\cdot \\ T(b_n) &= \alpha_{1,n}e_1 + \dots + \alpha_{m,n}e_m. \end{aligned}$$

[1]**Definition 274:** An $m \times n$ matrix A is nonsingular if for each $x \in F^n$, $Ax = 0$ implies that $x = 0$. We say $T \in \text{Hom}(V, W)$ is nonsingular if $\ker T = \{0\}$.

[1]**Proposition 275:** (Properties of M_{β}^{ξ})

- (1) M_{β}^{ξ} implements the action of T on basis vectors.
- (2) $M_{\beta}^{\xi}(T + U) = M_{\beta}^{\xi}(T) + M_{\beta}^{\xi}(U)$.
- (3) $M_{\beta}^{\xi}(rT) = rM_{\beta}^{\xi}(T)$.
- (4) M_{β}^{ξ} is one-to-one and onto.
- (5) T is nonsingular if and only if $M_{\beta}^{\xi}(T)$ is nonsingular.
- (6) $\dim(\text{Hom}(V, W)) = \dim V \cdot \dim W$.
- (7) If ξ, D , and β are bases for W, V , and U , then $M_{\beta}^{\xi}(T \circ S) = M_D^{\xi}(T)M_{\beta}^D(S)$.
- (8) Matrix multiplication is associative and distributive.
- (9) An $n \times n$ matrix is invertible if and only if it is nonsingular.
- (10) The map from $\text{Hom}(v,)$ to $n \times n$ matrices given by $T \mapsto M_{\beta}^{\beta}(T)$ is an algebra homomorphism and bijection.
- (11) Each column of $M_{\beta}^{\xi}(T)$ is the coefficients of $T(b_i)$ with respect to ξ , where $\beta = \{b_1, \dots, b_n\}$.
- (12) For $T \in \text{Hom}(V, U)$, column rank $M_{\beta}^{\xi}(T) = \dim T(V)$.

[1]**Definition 276:** We say two $n \times n$ matrices A and B are similar if there is an invertible $n \times n$ matrix P so that $B = P^{-1}AP$.

[1]**Theorem 277:** Two matrices are similar if and only if they are each a matrix of a common linear transformation with respect to two bases.

Dual Vector Spaces

[1]**Definition 278:** For any vector space V over a field F , we define the dual space of V to be $V^* := \text{Hom}(V, F) = \{f : V \rightarrow F : f \text{ is linear.}\}$.

[1]**Definition 279:** The dual basis $B^* = \{b_1, \dots, b_n\}$ is given by defining $b_i^*(b_i) = 1$ and $b_i^*(b_j) = 0$ for all $i \neq j$.

[1]**Definition 280:** The lattice, \mathcal{L} , of a finite vector space V is the set of all the subspaces of V with a partial ordering by inclusion. (We don't really need finite here.)

[1]**Proposition 281:** If $M, N \in \mathcal{L}(V)$, we have $M \cap N$ as the largest subspace contained in both M and N , and $M + N$ is the smallest subspace containing both.

[1]**Theorem 282:** (The Modular Condition) If $M \supseteq L$, then $M \cap (L + N) = (M \cap L) + (M \cap N)$ or $M \cap (L + N) = L + (M \cap N)$, and this is true in $\mathcal{L}(V)$.

[1]**Definition 283:** For $S \subseteq V^*$, $\text{Ann}(S)$ is the subspace of V given by $\text{Ann}(S) = \bigcap_{f \in S} \ker f = \{v \in V : f(v) = 0, \text{ for all } f \in S\}$.

[1]**Theorem 284:** We have a map $\text{Ann} : \mathcal{L}(V^*) \rightarrow \mathcal{L}(V)$, and it is an anti-isomorphism, i.e.

$$\begin{aligned} \text{Ann}(L + M) &= \text{Ann}(L) \cap \text{Ann}(M), \\ \text{Ann}(L \cap M) &= \text{Ann}(L) + \text{Ann}(M), \\ \text{Ann}(V^*) &= \{0\}, \\ \text{Ann}(\{0\}) &= V. \end{aligned}$$

It is bijective on the Lattice of Subspaces. Finally, if $\dim V < \infty$, $\dim(\text{Ann}(M)) = \dim V^* - \dim M$.

[1]**Definition 285:** The double dual of V is $V^{**} = (V^*)^* = \text{Hom}(\text{Hom}(V, F), F)$. If $\dim V < \infty$, $\dim V^{**} = \dim V^* = \dim V$. If $\dim V = \infty$, $\dim V^{**} > \dim V^* > \dim V$.

[1]**Theorem 286:** (Double Dual Theorem) The natural map $v \mapsto E_v$ is an injective vector space homomorphism. If $\dim V < \infty$, this map is an isomorphism.

[1]**Definition 287:** For each $T : V \rightarrow W$, there is a linear transformation $T^* : W^* \rightarrow V^*$ defined by $T^*(f) = f \circ T$.

[1]**Lemma 288:**

- (1) $\text{Ann}(\ker T^*) = T(V)$.
- (2) If $T : V \rightarrow W$ and $S : U \rightarrow V$, then $T \circ S : U \rightarrow W$ and $(T \circ S)^* = S^* \circ T^*$.
- (3) T and T^* have the same rank.

[1]**Theorem 289:** (Dual Transformation Theorem) If $T : V \rightarrow W$, β is a basis for V , and ξ is a basis for W , then $M_{\xi^*}^{\beta^*}(T)$ is the transpose of $M_{\beta}^{\xi}(T)$.

[1]**Corollary 290:** Row rank and column rank of an $m \times n$ matrix are equal.

[1]**Lemma 291:**

- (1) If $f \in V^*$ and $f \neq 0$, then $\ker f$ is a hyperplane.
- (2) Every hyperplane is the kernel of a nonsingular linear functional.
- (3) For $f, g \in V^*$, $\ker f \subseteq \ker g$ if and only if g is a scalar multiple of f .
- (4) For $f, g_1, \dots, g_n \in V^*$, f is a linear combination of g_1, \dots, g_n if and only if $\ker f \supseteq \bigcap_{i=1}^n \ker g_i$.

[2]**Definition 292:**

- (1) Let R be a commutative ring with identity and v_1, \dots, v_n, V, W be R -modules. A map $\varphi : V_1 \times V_2 \times \dots \times V_n \rightarrow W$ is called multilinear if for each fixed i and fixed elements $v_j \in V_j$, $j \neq i$, the map

$$V_i \rightarrow W \quad \text{defined by} \quad x \mapsto \varphi(v_1, \dots, v_{i-1}, x, v_{i+1}, \dots, v_n)$$

is an R -module homomorphism. If $V_i = V$ for $i = 1, 1, \dots, n$, then φ is called an n -multilinear function on V . If in addition, $W = R$, φ is called an n -multilinear form on V .

- (2) An n -multilinear function φ on V is called alternating if $\varphi(v_1, \dots, v_n) = 0$ whenever $v_i = v_{i+1}$ for some $i \in \{1, 2, \dots, n\}$. The function φ is called symmetric if interchanging v_i and v_j for any i and j in (v_1, \dots, v_n) does not alter the value of φ on this n -tuple.

[2]**Proposition 293:** Let φ be an n -multilinear alternating function on V . Then

- (1) $\varphi(v_1, \dots, v_{i-1}, v_{i+1}, v_i, v_{i+2}, \dots, v_n) = -\varphi(v_1, \dots, v_n)$ for any $i \in \{1, \dots, n-1\}$
- (2) For each $\sigma \in S_n$, $\varphi(v_{\sigma(1)}, \dots, v_{\sigma(n)}) = \epsilon(\sigma)\varphi(v_1, \dots, v_n)$, where $\epsilon(\sigma)$ is the sign of the permutation σ .
- (3) If $v_i = v_j$ for any pair of distinct, $i, j \in \{1, \dots, n\}$, then $\varphi(v_1, \dots, v_n) = 0$.
- (4) If v_i is replaced by $v_i + \alpha v_j$ in v_1, \dots, v_n for any $j \neq i$ and any $\alpha \in R$, the value of φ on this n -tuple is not changed.

[2]**Proposition 294:** Assume φ is an n -multilinear alternating function on V and that for some v_1, \dots, v_n and $w_1, \dots, w_n \in V$ and some $\alpha_{ij} \in R$ we have

$$\begin{aligned} w_1 &= \alpha_{11}v_1 + \dots + \alpha_{n1}v_n, \\ w_2 &= \alpha_{12}v_1 + \dots + \alpha_{n2}v_n, \\ &\vdots \\ &\vdots \\ &\vdots \\ w_n &= \alpha_{1n}v_1 + \dots + \alpha_{nn}v_n. \end{aligned}$$

Then,

$$\varphi(w_1, \dots, w_n) = \sum_{\sigma \in S_n} \epsilon(\sigma)\alpha_{\sigma(1)1} \dots \alpha_{\sigma(n)n} \varphi(v_1, \dots, v_n).$$

[2]**Definition 295:** An $n \times n$ determinant function on R is any function $\det : M_{n \times n}(R) \rightarrow R$ that satisfies the following two axioms:

- (1) \det is an n -multilinear alternating form on R^n , where the n -tuples are the n columns of the matrices in $M_{n \times n}(R)$.
- (2) $\det(I) = 1$

[2]**Theorem 296:** (The Determinant Theorem) There is a unique $n \times n$ determinant function on R and it can be computed for any $n \times n$ matrix (α_{ij}) by the formula

$$\det(\alpha_{ij}) = \sum_{\sigma \in S_n} \epsilon(\sigma)\alpha_{\sigma(1)1} \dots \alpha_{\sigma(n)n}.$$

[2]**Corollary 297:** The determinant is an n -multilinear function of the rows of $M_{n \times n}(R)$ and for any $n \times n$ matrix A , $\det A = \det(A^t)$, where A^t is the transpose of A .

[2]**Theorem 298:** (Cramer's Rule) If A_1, \dots, A_n are the columns of an $n \times n$ matrix A and $B = \beta_1 A_1 + \dots + \beta_n A_n$, for some $\beta_1, \dots, \beta_n \in R$, then

$$\beta_i \det A = \det(A_1, \dots, A_{i-1}, B, A_{i+1}, \dots, A_n).$$

[2]**Corollary 299:** If R is an integral domain, then $\det A = 0$ for $A \in M_n(R)$ if and only if the columns of A are R -linearly dependent as elements of the free R -module of rank n . Also, $\det A = 0$ if and only if the rows of A are R -linearly dependent.

[2]**Theorem 300:** For matrices $A, B \in M_{n \times n}(R)$, $\det AB = (\det A)(\det B)$.

Structure Theorem for Finitely Generated Modules over a PID

[1]**Definition 301:** Let R be a ring and M be a left R -module. We say M is Noetherian if any increasing chain of submodules is eventually constant, i.e. $M_1 \subseteq M_2 \subseteq \dots$ implies there exists J such that for all $i \geq J$, $M_i = M_J$.

[1]**Theorem 302:** For a left R -module M , TFAE:

- (1) M is Noetherian.
- (2) Any nonempty collection of submodules of M has a maximal element.
- (3) Every submodules of M is finitely generated.

[1] **Corollary 303:**

- (1) PID's are Noetherian.
- (2) Any nonempty collection of ideals of a PID has a maximal element.

[1] **Proposition 304:** Let R be an integral domain and M be a free R -module of rank $n \in \mathbb{N}$. Then any $n + 1$ elements of M are R -linearly dependent.

[1] **Definition 305:** Let R be an integral domain and M be an R -module. $\text{Tor}(M) = \{x \in M : rx = 0 \text{ for some } r \in R \setminus \{0\}\}$. Submodules of $\text{Tor}(M)$ are called torsion modules of M . If $\text{Tor}(M) = \{0\}$, then M is torsion free.

[1] **Definition 306:** If N is a submodule of M as above, then $\text{Ann}(N) = \{r \in R : rn = 0 \text{ for all } n \in N\}$.

[1] **Lemma 307:**

- (1) If $L \subseteq N$, then $\text{Ann}(L) \supseteq \text{Ann}(N)$.
- (2) Let M be an R -module, and L, N be submodules of M . Assume R is a PID, $\text{Ann}(L) = (b)$ and $\text{Ann}(N) = (a)$. If $N \subseteq L$, then $a|b$.

[1] **Definition 308:** The rank of a module is the maximum number of R -linearly independent elements.

[1] **Lemma 309:**

- (1) If R is a field, rank is the same as dimension.
- (2) If N is a submodules of M , then $\text{rank } N \leq \text{rank } M$, provided M is free and R is an integral domain.

[1] **Theorem 310:** (Free Basis Theorem) Let R be a PID, M be a free R -module of rank $n \in \mathbb{N}$, and N be a submodule of M . Then

- (1) N is free and $\text{rank } N$, call it m , has $m \leq n$.
- (2) There is a basis y_1, \dots, y_n of M and $a_1, \dots, a_m \in R \setminus \{0\}$ so that
 - (a) $a_1 y_1, \dots, a_m y_m$ is a basis of N .
 - (b) $a_1 | a_2, a_2 | a_3, \dots, a_{m-1} | a_m$.

[1] **Proposition 311:** For a cyclic R -module, M , with generator x , i.e. $M = Rx$, if $\pi(r) = rx$, then $\pi \in \text{Hom}(R, M)$ and $M \cong R/\ker \pi$. If R is a PID, $\ker \pi = (a)$, and so $M \cong R/(a)$.

[1] **Theorem 312:** (Invariant Factor Form of the Fundamental Structure Theorem) Let M be a finitely generated module over a PID R . Then

$$M \cong R^r \oplus R/(a_1) \oplus \dots \oplus R/(a_m),$$

where $r \geq 0, a_1, \dots, a_m \in R \setminus \{0\}$, and $a_1 | a_2, \dots, a_{m-1} | a_m$. Furthermore, M is torsion free if and only if M is free if and only if $m = 0$. Also,

$$\text{Tor}(M) \cong R/(a_1) \oplus \dots \oplus R/(a_m),$$

and if $r = 0$, $\text{Ann}(M) = (a_m)$.

[1] **Definition 313:** We call r the free rank of M , and we call a_1, a_2, \dots, a_m the invariant factors of M .

[1] **Lemma 314:** Both as rings and as R -modules, we have the following:

$$R/(a) \cong R/(p_1^{\alpha_1}) \oplus \dots \oplus R/(p_n^{\alpha_n}),$$

where $a = up_1^{\alpha_1} \dots p_n^{\alpha_n}$.

[1]**Theorem 315:** (Elementary Divisor Form of the Fundamental Structure Theorem) Let M be a finitely generated module over a PID. Then

$$M \cong R^r \oplus R/(p_1^{\alpha_1}) \oplus \cdots \oplus R/(p_n^{\alpha_n}),$$

where the p_i 's are primes in R and $\alpha_i \geq 1$ for all $1 \leq i \leq n$.

[1]**Definition 316:** We call $p_1^{\alpha_1}, \dots, p_t^{\alpha_t}$ as above the elementary divisors of M .

[1]**Theorem 317:** (Primary Decomposition Theorem) Let M be a nonzero torsion module over a PID with $\text{Ann}(M) = (a)$. If a factors as $a = up_1^{\alpha_1} \cdots p_n^{\alpha_n}$ for distinct primes p_1, \dots, p_n , then let $N_i = \{x \in M : p_i^{\alpha_i}x = 0\}$ for $1 \leq i \leq n$. Then N_i is a submodule of M with $\text{Ann}(N_i) = (p_i^{\alpha_i})$ and $M \cong N_1 \oplus N_2 \oplus \cdots \oplus N_n$.

[1]**Proposition 318:** If $M_1 \cong M_2$, then free rank, invariant factors, and elementary divisors are all the same in M_1 and M_2 .

Rational Canonical Form

[1]**Definition 319:** (Structure of $F[x]/a(x)$) Let $a(x) = x^k + b_{k-1}x^{k-1} + \cdots + b_1x + b_0$. Then the companion matrix, denoted by $C_{a(x)}$ is given by

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & -b_0 \\ 1 & 0 & \cdots & 0 & 0 & -b_1 \\ 0 & 1 & \cdots & 0 & 0 & -b_2 \\ \vdots & & & & & \vdots \\ 0 & 0 & \cdots & 0 & 1 & -b_{k-1} \end{pmatrix}$$

[1]**Theorem 320:** (RCF Theorem-Rational Canonical Form) For every linear transformation T on a finite dimensional vector space V ,

- (1) There is a basis β such that the matrix of T with respect to this basis is in rational canonical form, i.e. it is blockdiagonal with the companion matrix for each $a_i(x)$ from the structure theorem down the diagonal and zeros everywhere else. Here each $a_i(x)$ is monic and $a_1(x)|a_2(x), \dots, a_{m-1}(x)|a_m(x)$.
- (2) This matrix is unique. So we will use $RCF(T)$ to denote this matrix.

[1]**Theorem 321:** For a finite dimensional vector space, V , and $S, T \in \text{Hom}(V, V)$, TFAE:

- (1) $S \sim T$.
- (2) The $F[x]$ -modules on V from S and T are isomorphic.
- (3) $RCF(S) = RCF(T)$.

[1]**Corollary 322:** If $A, B \in M_n(F)$ and F is a subfield of K , then $RCF(A)$ [in $M_n(F)$] and $RCF(A)$ [in $M_n(K)$] are the same, and $A \sim B$ [in $M_n(F)$] if and only if $A \sim B$ [in $M_n(K)$].

[1]**Definition 323:** For $A \in M_n(F)$, the characteristic polynomial of A , $c_A(x) \in F[x]$, is $\det(xI - A)$. Also, the minimal polynomial of A , $m_A(x)$, is the monic generator of $\text{Ann}(V)$, where V is the vector space F^n with the $F[x]$ -module structure from A .

[1]**Theorem 324:** (Cayley-Hamilton Theorem) As $c_A(A) = 0$, $m_A(x)|c_A(x)$.

[1]**Theorem 325:** (Smith Normal Form of a Matrix) For $A \in M_n(F)$, if we use row and column operations to reduce $xI - A$ to a matrix with only 1's followed by the $a_i(x)$'s down the diagonal and zeros everywhere else with $a_1(x)|a_2(x), \dots, a_{m-1}(x)|a_m(x)$, then the $a_i(x)$'s are the invariant factors of A .

[1]**Theorem 326:** (Jordan Canonical Form) For $A \in M_n(F)$ so that $c_A(x)$ factors completely, A is similar to a matrix in Jordan Canonical form, and this matrix is unique up to some permutation of the diagonal blocks.

[1]**Corollary 327:**

- (1) If $A \sim D$, a diagonal matrix, then $JCF(A) = D$ up to a permutation of the diagonal elements.
- (2) Diagonal matrices are similar if and only if diagonal entries are equal upto a permutation.

[1]**Corollary 328:** If $A \in M_n(F)$ and $c_A(x)$ factors completely, then A is similar to a diagonal matrix if and only if $m_A(x)$ has no repeated roots.

Field Theory

[1]**Definition 329:** The characteristic of a field F is the smallest positive integer p such that $p \cdot 1 = 0$, if one exists. Otherwise, the characteristic is zero.

[1]**Definition 330:** The prime subfield of a field F is the subfield generated by 1_F .

[1]**Proposition 331:** If $\text{char } F = 0$, the prime subfield is \mathbb{Q} . If $\text{char } F = p$, then the prime subfield is $\mathbb{Z}/p\mathbb{Z}$.

[1]**Definition 332:** If F is a subfield of K , then we call K an extension of F . We write K/F to say K is an extension of F . We use $[K : F]$ for the index of K over F , $\dim_F(K)$.

[1]**Proposition 333:** If $\varphi : F \rightarrow F'$ is a field homomorphism, then $\varphi(F)$ either is zero or is isomorphic to F .

[1]**Theorem 334:** (Adding a Root Theorem) Let F be a field and $p(x) \in F[x]$ be irreducible. There is an extension K/F so that $p(x)$ has a root in K , i.e. there exists $\alpha \in K$ such that $p(\alpha) = 0$.

[1]**Theorem 335:** In the above context, if $\deg p(x) = n$ and $\theta = x + (p(x)) \in K$, then $\{1, \theta, \dots, \theta^{n-1}\}$ is a basis for K as a vector space over F , i.e. $[K : F] = n$.

[1]**Definition 336:** Let K be an extension of F and $\{\alpha_i : i \in I\} \subseteq K$. The smallest subfield containing F and all the α_i is called the subfield generated by $\{\alpha_i : i \in I\}$ over F .

[1]**Definition 337:** For K/F , we call K a simple extension if there is $\alpha \in K$ so that K is the subfield generated by α over F . We call α a primitive element of K/F .

[1]**Theorem 338:** Let F be a field and $p(x) \in F[x]$ be irreducible. Let K be an extension of F so that $p(x)$ has a root $\alpha \in K$. Then the subfield generated by α , $F(\alpha)$, is isomorphic to $F[x]/(p(x))$.

[1]**Theorem 339:** Let F be a field, and $p(x) \in F[x]$ be irreducible. Suppose K is an extension of F with $\alpha \in K$ such that $p(\alpha) = 0$. Then $F(\alpha) \cong F[x]/(p(x))$.

[1]**Theorem 340:** Suppose $\varphi : F \rightarrow G$ is a field isomorphism, $p(x) \in F[x]$ is irreducible, $q(x) \in G[x]$ is the image of $p(x)$ under the natural isomorphism. If α is a root of $p(x)$ in some extension of F , and β is a root of $q(x)$ in some extension G , then there is a field isomorphism $\sigma : F(\alpha) \rightarrow G(\beta)$ with $\sigma|_F = \varphi$.

[1]**Definition 341:** For K an extension of F and $\alpha \in K$ satisfies $p(\alpha) = 0$ for some $p(x) \in F[x]$, then α is algebraic over F . If there is no such p , α is transcendental over F .

[1]**Proposition 342:** If $\alpha \in K$ is algebraic over F , then there is a unique polynomial $m_\alpha(x) \in F[x]$, monic and irreducible, so that $m_\alpha(\alpha) = 0$. Moreover, for all $p \in F[x]$ so that $p(\alpha) = 0$, $m_\alpha | p$.

[1]**Definition 343:** We call $M_\alpha(x)$ the minimal polynomial of α over F .

[2]**Corollary 344:** If L/F is an extension of fields and α is algebraic over both F and L , then $m_{\alpha,L}(x)$ divides $m_{\alpha,F}(x)$ in $L[x]$.

[2]**Definition 345:** The polynomial $m_{\alpha,F}(x)$ in Proposition 342 is called the minimal polynomial for α over F . The degree of $m_\alpha(x)$ is called the degree of α .

[2]**Proposition 346:** Let α be algebraic over the field F and let $F(\alpha)$ be the field generated by α over F . Then $F(\alpha) \cong F[x]/(m_\alpha(x))$ so that in particular $[F(\alpha) : F] = \deg m_\alpha(x) = \deg \alpha$.

[2]**Proposition 347:** The element α is algebraic over F if and only if the simple extension $F(\alpha)/F$ is finite. More precisely, if α is an element of an extension of degree n over F , then α satisfies a polynomial of degree at most n over F and if α satisfies a polynomial of degree n over F , then the degree of $F(\alpha)$ over F is at most n .

[2]**Corollary 348:** If the extension K/F is finite, then it is algebraic.

[2]**Theorem 349:** Let $F \subseteq K \subseteq L$ be fields. Then $[L : F] = [L : K][K : F]$.

[2]**Corollary 350:** Suppose L/F is a finite extension and let K be any subfield of L containing F , $F \subseteq K \subseteq L$. Then $[K : F]$ divides $[L : F]$.

[2]**Definition 351:** An extension K/F is finitely generated if there are elements $\alpha_1, \alpha_2, \dots, \alpha_k \in K$ such that $K = F(\alpha_1, \dots, \alpha_k)$.

[2]**Lemma 352:** $F(\alpha, \beta) = (F(\alpha))(\beta)$.

[2]**Theorem 353:** The extension K/F is finite if and only if K is generated by a finite number of algebraic elements over F . More precisely, a field generated over F by a finite number of algebraic elements of degrees n_1, n_2, \dots, n_k is algebraic of degree less than or equal to $n_1 n_2 \cdots n_k$.

[2]**Corollary 354:** Suppose α and β are algebraic over F . Then $\alpha \pm \beta, \alpha\beta, \alpha/\beta$ are all algebraic.

[2]**Corollary 355:** Let L/F be an arbitrary extension. Then the collection of elements of L that are algebraic over F form a subfield K of L .

[2]**Theorem 356:** If K is algebraic over F and L is algebraic over K , then L is algebraic over F .

[2]**Definition 357:** Let K_1 and K_2 be two subfields of a field K . Then the composite field of K_1 and K_2 , denoted K_1K_2 , is the smallest subfield of K containing both K_1 and K_2 . Similarly, the composite of any collection of subfields of K is the smallest subfield containing all the subfields.

[2]**Proposition 358:** Let K_1 and K_2 be two finite extensions of a field F contained in K . Then $[K_1K_2 : F] \leq [K_1 : F][K_2 : F]$ with equality if and only if an F -basis for one of the fields remains linearly independent over the other field. If $\alpha_1, \dots, \alpha_n$ and β_1, \dots, β_m are bases for K_1 and K_2 over F , respectively, then the elements $\alpha_i\beta_j$ for $i = 1, 2, \dots, n$ and $j = 1, 2, \dots, m$ span K_1K_2 over F .

[2]**Corollary 359:** Suppose that $[K_1 : F] = n, [K_2 : F] = m$ in Proposition 21, where n and m are relatively prime. Then $[K_1K_2 : F] = [K_1 : F][K_2 : F]$.

Splitting Fields

[1]**Definition 360:**

- (1) We say a polynomial $p(x)$ splits completely over K if it factors into linear factors in $K[x]$.
- (2) We say a field extension K/F is splitting field for $p(x) \in F[x]$ if
 - (a) $p(x)$ splits completely over K .
 - (b) $p(x)$ does not split completely over any proper subfield of K containing F .

[1]**Theorem 361:** For any field F and any polynomial $p(x) \in F[x]$, there is an extension of F that is a splitting field for $p(x)$.

[1]**Corollary 362:** If K is the splitting field of $p(x) \in F[x]$ over F , and $\deg p(x) = n$, then $[K : F] \leq n$.

[1]**Definition 363:** We call an n^{th} root of unity primitive if it generates the group of n^{th} roots of unity. We call $\mathbb{Q}(\zeta_n)$ the cyclotomic field of the n^{th} roots of unity, where $\zeta_n = e^{2\pi i/n}$.

[1]**Theorem 364:** If $\varphi : F \rightarrow F'$ is a field isomorphism and E and E' are splitting fields for $p \in F[x]$ and $p' \in F'[x]$ with p' the image of p under the natural extension of φ , then there is a field isomorphism $\Phi : E \rightarrow E'$ so that $\Phi|_F = \varphi$.

[1]**Corollary 365:** Splitting fields are unique upto isomorphism.

[1]**Definition 366:** Let $\text{Aut}(K)$ be the group of all field isomorphisms $\sigma : K \rightarrow K$. If K is an extension of F , the $\text{Aut}(K/F)$ is the subgroup of all $\sigma \in \text{Aut}(K)$ so that $\sigma(f) = f$ for all $f \in F$.

[1]**Proposition 367:** If $\alpha \in K$ is algebraic over F , then for each $\sigma \in \text{Aut}(K/F)$, $\sigma(\alpha)$ is a root of the minimal polynomial for α over F .

[1]**Lemma 368:** If $F_1 \subseteq F_2 \subseteq K$ are all fields, then $\text{Aut}(K/F_1) \geq \text{Aut}(K/F_2)$.

[1]**Proposition 369:** Given a subgroup H of $\text{Aut}(K/F)$, consider the set of all elements of K , k , such that $\sigma(k) = k$ for all $\sigma \in H$. This set is a subfield of K containing F .

[1]**Definition 370:** We call the subfield in the previous proposition the fixed subfield of H , and denote it F_H .

[1]**Remark:** If $H_1 \leq H_2 \leq \text{Aut}(K/F)$, then the fixed field of H_1 contains the fixed field of H_2 .

[1]**Theorem 371:** For any finite extension K/F , $|\text{Aut}(K/F)| \leq [K : F]$.

[1]**Definition 372:** We say K is Galois over F or K is a Galois extension of F if $|\text{Aut}(K/F)| = [K : F]$. In this case, we call $\text{Aut}(K/F)$ the Galois group of K over F and use $\text{Gal}(K/F)$ for it.

[1]**Theorem 373:** For an extension K/F , TFAE:

- (1) K is Galois over F .
- (2) K is the splitting field of some polynomial over F .
- (3) The fixed field of $\text{Aut}(K/F)$ is exactly F .

[1]**Theorem 374:** (Fundamental Theorem of Galois Theory) If K/F is Galois, there is a bijection between subfields of K containing F and subgroups of $\text{Aut}(K/F)$ given by $E \mapsto \{\sigma \in \text{Aut}(K/F) : \sigma(e) = e, \text{ for all } e \in E\}$, with inverse $H \mapsto F_H$. Moreover, these maps are

- (1) inclusion reversing
- (2) $[K : E] = |H|$ and $[E : F] = [\text{Aut}(K/F) : H]$, where the RHS denotes the number of left cosets of H in $\text{Aut}(K/F)$.

- (3) K is Galois over E .
- (4) E is Galois over F if and only if H is normal.
- (5) If E_1, E_2 are subfields of $K \supseteq F$ with corresponding subgroups H_1 and H_2 , then $E_1 \cap E_2$ corresponds to the subgroup generated by H_1 and H_2 and $E_1 E_2$ corresponds to $H_1 \cap H_2$.

References

- [1] Allan Donsig. Math 817 notes. Fall 2011.
- [2] David S. Dummit and Richard M. Foote. *Abstract algebra*. John Wiley & Sons Inc., Hoboken, NJ, third edition, 2004.