1. **Groups and Basic Properties (by Derrek Yager)**

- An operation is a function from a set $A$ to a set $B$ and is a rule that assigns each element of $A$ to exactly one element of $B$.

  For example, in the operation $*: G \times G \rightarrow G$, if we let $a, b \in G$, then $(a, b) \mapsto a \ast b$.

- A group $G$ is simply a nonempty set $G$ under a closed operation $*$ where the following properties are satisfied:
  1. **Associativity.** For $a, b, c \in G, a \ast (b \ast c) = (a \ast b) \ast c$.
  2. **Identity.** There exists $e \in G$ such that $a \ast e = e \ast a = a$.
  3. **Inverses.** For all $a \in G$, $\exists a^{-1} \in G$ such that $a \ast a^{-1} = a^{-1} \ast a = e$.

**Examples of Groups**

<table>
<thead>
<tr>
<th>Group</th>
<th>Form of Element</th>
<th>Identity</th>
<th>Inverse</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\langle \mathbb{Z}, + \rangle$</td>
<td>$a$</td>
<td>0</td>
<td>$-a$</td>
</tr>
<tr>
<td>$\langle \mathbb{Q}, + \rangle$</td>
<td>$a/b$</td>
<td>0</td>
<td>$-a/b$</td>
</tr>
<tr>
<td>$\langle \mathbb{Q} - {0}, \ast \rangle$</td>
<td>$a$</td>
<td>1</td>
<td>$1/a$</td>
</tr>
<tr>
<td>$\langle \mathbb{Z}_n, + \rangle$</td>
<td>$0 \leq a \leq n - 1$</td>
<td>0</td>
<td>$n - a$</td>
</tr>
</tbody>
</table>

- For an example of the $\langle \mathbb{Z}_n, + \rangle$ group, consider the following Cayley table representing $\langle \mathbb{Z}_5, + \rangle$:

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

- A group $G$ is considered abelian if $a \ast b = b \ast a \ \forall \ a, b \in G$. So far, all of the group examples have been abelian.

  One non-abelian group is $GL(2, \mathbb{R})$, which is all $2 \times 2$ matrices with real entries and nonzero determinants.

  Another non-abelian group consists of the Quaternions $\{1, -1, i, -i, j, -j, k, -k\}$ where $i^2 = j^2 = k^2 = -1$. Also, they must satisfy

  $i \cdot j = k \quad j \cdot i = -k$

  $j \cdot k = i \quad k \cdot j = -i$

  $k \cdot i = j \quad i \cdot k = -j$

  Yet another non-abelian group consists of $D_n$. When $n = 4$, this group represents the symmetries on a square.
There are also four key properties of groups.

1. In every group there exists one unique identity element.
   \[\text{Proof.}\] By contradiction, let \(e\) and \(e'\) be two distinct identity elements in a group \(G\). By definition, \(e'e = e'\) since \(e\) is an identity element, but we also have \(e'e = e\) since \(e'\) is an identity element. Thus, we have \(e' = e'e = e\) which contradicts our statement that \(e\) and \(e'\) are distinct. Hence, the identity element is unique. (Fun Fact! The tendency to use \(e\) to represent the identity element roots from the German word "Einheit") □

2. In every group, right and left cancellation laws hold.
   \[\text{Proof.}\] Let \(a, b, c \in G\) such that \(a^{-1}, b^{-1} \in G\) by definition of groups. If \(ab = ac\), then
   \[
   a^{-1}ab = a^{-1}ac \\
   eb = ec \\
   b = c
   \]
   By symmetry, the right cancellation law holds such that \(ab = cb\) implies \(a = c\). □

3. If \(G\) is a group, with \(a, b \in G\) and \(ab = e\), then \(a = b^{-1}\) and \(b = a^{-1}\).
   \[\text{Proof.}\] For showing \(a = b^{-1}\), we see that
   \[
   ab = e \\
   a^{-1}ab = a^{-1}e \\
   eb = a^{-1} \\
   b = a^{-1}
   \]
   For showing \(b = a^{-1}\), we also see that
   \[
   ab = e \\
   abb^{-1} = eb^{-1} \\
   ae = b^{-1} \\
   a = b^{-1}
   \]

4. If \(G\) is a group with \(a, b \in G\), then \((ab)^{-1} = b^{-1}a^{-1}\).
   \[\text{Proof.}\] We see this to be obviously true with
   \[
   (ab)(ab)^{-1} = (ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e.
   \]
   Thus, the given inverse achieves its purpose. □

Stay tuned for the next exciting part of the series... Permutations!

\[\sim\]
\[\bigcirc \bigcirc\]
\[\sim\]
\[\infty\]

2. PERMUTATIONS (BY ANNE HO)

**Definition.** A function \(f : X \to Y\) is **injective** if for every \(x_1, x_2 \in X\), when \(f(x_1) = f(x_2), x_1 = x_2\). A function \(f : X \to Y\) is **surjective** if for every \(y \in Y\), there exists an \(x \in X\) such that \(f(x) = y\). A function \(f : \to Y\) is **bijective** if it is both injective and surjective.

**Definition.** A function is a **permutation** if it is a bijection onto itself \(f : X \to X\). Notation: \(X = \{1, 2, \ldots n\}\).
\[
\alpha = \begin{pmatrix}
1 & 2 & \cdots & n \\
\alpha(1) & \alpha(2) & \cdots & \alpha(n)
\end{pmatrix}
\]

**Definition.** \(S_n\) is the group of permutations called the **symmetric group**.
Example. Suppose $X = \{1, 2, 3, 4\}$ and $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$.

$\alpha \in S_4$, the set of permutations on $X$, and $\alpha(1) = 3, \alpha(2) = 1, \alpha(3) = 4, \alpha(4) = 2$.

Suppose $X = \{1, 2, 3, 4\}$ and $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$.

$\beta \in S_4$ as well.

Composing $\alpha \circ \beta(1)$, we get $\alpha(2) = 1$.

Example. Let $X = \{1, 2, 3\}$. We list the elements of $S_3$:

$I = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$

$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

$\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

$\gamma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

$\delta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

$\mu = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

Example. Consider the Dihedral Group, $D_4$.

The identity is $I = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$

A rotation of 90-degrees would be: $R_{90} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$

We can do this for the other rotations and flips about various axes too: $R_{180}, R_{270}, H, V, D_1, D_2$.

Definition. If $\alpha \in S_n$ and $i \in \{1, 2, ..., n\}$, then $\alpha$ fixes $i$ if $\alpha(i) = i$. $\alpha$ moves $i$ if $\alpha(i) \neq i$.

Definition. Let $i_1, i_2, ..., i_r$ be elements in $X = \{1, 2, ..., n\}$. If $\alpha \in S_n$ fixes the other integers, and if $\alpha(i_1) = i_2, \alpha(i_2) = i_3, ..., \alpha(i_{r-1}) = i_n$ and $\alpha(i_r) = i_1$, then $\alpha$ is called an $r$-cycle. A 2-cycle is called a transposition. A 1-cycle is just the identity.

Example. $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 5 \end{pmatrix} = (1 \ 4 \ 5 \ 2)$

Example. $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 5 \end{pmatrix} = (1 \ 2 \ 3 \ 4) (5) = (1 \ 2 \ 3)$

Example. Write as a product of disjoint cycles. $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 4 & 7 & 2 & 5 & 1 & 8 & 9 & 3 \end{pmatrix}$

$= (1 \ 6) (2 \ 4) (3 \ 7 \ 8 \ 9) (5)$
Example. Product of Permutations. \( \alpha = (1 \ 2) (1 \ 3 \ 4 \ 2 \ 5) (2 \ 5 \ 1 \ 3) \)

We see that:
1 \rightarrow 3 \rightarrow 4
2 \rightarrow 5 \rightarrow 1 \rightarrow 2
3 \rightarrow 2 \rightarrow 5
4 \rightarrow 2 \rightarrow 1
5 \rightarrow 1 \rightarrow 3

So we have: \( \alpha = (1 \ 4) (2) (3 \ 5) = (1 \ 4) (3 \ 5) \)

Definition. Two cycles \( \alpha = (a_1 a_2 ... a_m) \) and \( \beta = (b_1 b_2 ... b_m) \) are disjoint if \( a_i \neq b_j \) for all \( i, j \).

Lemma 2.1. Disjoint cycles \( \alpha, \beta \in S_n \) commute.

Note. Every permutation is a product of disjoint cycles.

Theorem 2.2. (1) The inverse of \((i_1, i_2, ..., i_r)\) is the \( r \)-cycle \((i_r, i_{r-1}, ..., 1)\).

(2) If \( \alpha = \beta_1 \beta_2 ... \beta_t \) is a product of disjoint cycles, then \( \alpha^{-1} = \beta_1^{-1} \beta_2^{-1} ... \beta_t^{-1} \).

Proof. (1) Consider \((i_1, i_2, ..., i_r)(i_r, i_{r-1}, ..., 1)\).

We see that:
\( i_1 \rightarrow i_r \rightarrow i_1 \)
\( i_2 \rightarrow i_1 \rightarrow i_2 \)
\( ... \)
\( i_{r-1} \rightarrow i_{r-2} \rightarrow i_{r-1} \)
\( i_r \rightarrow i_{r-1} \rightarrow i_r \)

So \((i_1, i_2, ..., i_r)(i_r, i_{r-1}, ..., 1) = (1)\)

Similarly, \((i_r, i_{r-1}, ..., 1)(i_1, i_2, ..., i_r) = (1)\).

(2) Consider \((\beta_1 \beta_2 ... \beta_t)(\beta_t^{-1} \beta_{t-1}^{-1} ... \beta_1^{-1})\).

We see that \( \beta_t \beta_t^{-1} = 1 \), \( \beta_{t-1} \beta_{t-1}^{-1} = 1 \) and so on. Thus we have 1.

Similarly, \((\beta_t^{-1} \beta_{t-1}^{-1} ... \beta_1^{-1})(\beta_1 \beta_2 ... \beta_t) = 1\).

Since \( \alpha = \beta_1 \beta_2 ... \beta_t \), then \( \alpha^{-1} = \beta_t^{-1} \beta_{t-1}^{-1} ... \beta_1^{-1} \). From the Lemma, we know that \( \alpha^{-1} = \beta_1^{-1} \beta_2^{-1} ... \beta_t^{-1} \).

\[ \square \]

Note. If \( n \geq 2 \), then every \( \alpha \in S_n \) is a product of transpositions. To check this, consider:
\((1 \ 2 \ ... \ r) = (1 \ r)(1 \ r - 1) ... (1 \ 3)(1 \ 2)\)

We see that:
1 \rightarrow 2
2 \rightarrow 1 \rightarrow 3
3 \rightarrow 1 \rightarrow 4
\( ... \)
\( r - 1 \rightarrow 1 \rightarrow r \)

Definition. A permutation is even if it can be factored into a product of an even number of transpositions; otherwise, it is odd. The parity of a permutation is whether it is even or odd.

Example. \( \alpha = (1 \ 2 \ 3) = (1 \ 3) (1 \ 2) \) So it is even.

\(^1\)Due to some confusion during the lecture, this definition was later added to these notes and is from Durbin’s *Modern Algebra*, Fifth Edition.
Definition. A subset $H$ of a group $G$ is a subgroup of $G$ if the following axioms hold:

(i) $1 \in H$
(ii) If $x, y \in H$, then $xy \in H$ (closure)
(iii) If $x \in H$, then $x^{-1} \in H$ (inverses).

Example. Let $G = \mathbb{R}^* = \mathbb{R} \setminus \{0\}$ and $H = \{2^n : n \in \mathbb{Z}\}$. Show that $<H, \cdot>$ is a subgroup of $<G, \cdot>$.

(i) $2^0 = 1$, so $1 \in H$
(ii) Let $x, y \in H$ such that $x = 2^n$ and $y = 2^m$. Then $xy = 2^n2^m = 2^{n+m}$. Since $n + m \in \mathbb{Z}$, $xy \in H$.
(iii) Let $x \in H$ such that $x = 2^n$. Then $x^{-1} = 2^{-n}$ because $2^n2^{-n} = 1$.

Theorem 3.1. Let $G$ be a group and $H$ a nonempty subset of $G$. If $a, b \in H$ implies $ab^{-1} \in H$, then $H$ is a subgroup of $G$.

Proof. (i) Since $H$ is nonempty, choose $x \in H$. Let $a = b = x$. Then $ab^{-1} = xx^{-1} = 1$. So $1 \in H$.
(ii) Let $a = e \in H$, $b = x$. Then $ab^{-1} = ex^{-1} = x^{-1}$. So $x^{-1} \in H$.
(iii) Let $a = x, b = y^{-1}$ for $x, y \in H$. Then $xy = x(y^{-1})^{-1} = ab^{-1} \in H$. \(\square\)

Example. Let $<G, \cdot>$ be an abelian group. Show $H = \{x^2 | x \in G\}$ is a subgroup of $G$.

Let $a^2, b^2 \in H$. Then $a^2(b^2)^{-1} = a^2b^{-2} = ab^{-1}ab^{-1} = (ab^{-1})^2 \in H$.

Definition. The order of an element $g \in G$, denoted $|g|$, is the smallest positive integer $n$ such that $g^n = 1$. If no such integer exists, we say that $g$ has infinite order.

Example. $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$

$|0| = 1 \quad |1| = 6 \quad |2| = 3 \quad |3| = 2 \quad |4| = 3 \quad |5| = 6$

Example. $U(10) = \{k | \gcd(k, 10) = 1\} = \{1, 3, 7, 9\}$. With $* = \cdot \mod 10$.

$|1| = 1 \quad |3| = 4 \quad |7| = 4 \quad |9| = 2$

Definition. Let $<a>$ denote the set $\{a^n : n \in \mathbb{Z}\}$.

Theorem 3.2. Let $G$ be a group, and let $a \in G$. Then $<a>$ is a subgroup of $G$.

Proof. Prove in homework. \(\square\)

Example. $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$

$<0> = \{0\} \quad <1> = \mathbb{Z}_6 \quad <2> = \{0, 2, 4\} \quad <3> = \{0, 3\}$

The order of the element is equal to the order of the subgroup generated by the element. $|a| = |<a>|$.

Definition. The center $Z(G)$ of a group $G$ is the subset of elements in $G$ that commute with every other element in $G$. Symbolically, $Z(G) = \{a \in G | ag = ga \forall g \in G\}$.

Theorem 3.3. The center of a group $G$ is a subgroup of $G$.

Proof. Prove in homework. \(\square\)

Definition. A group $G$ is called cyclic if there is an element $a$ such that

$G = \{a^n | n \in \mathbb{Z}\}$.

The element $a$ is called the generator.

Example. $\mathbb{Z}_n = \{0, 1, \cdots, n-1\}$ is always generated by 1 or $n-1$, and may be generated by other numbers also. For instance, $\mathbb{Z}_8 = \{1, 7, 3, 5\}$.

Example. $U(8) = \{1, 3, 5, 7\}$

$|1| = 1 \quad |3| = 2 \quad |5| = 2 \quad |7| = 2$
Theorem 3.4. Let $G$ be a group and $a \in G$.

(i) If $a$ has infinite order, then $a^i = a^j$ iff $i = j$.
(ii) If $a$ has finite order $n$, then $<a> = \{e, a, a^2, \ldots, a^{n-1}\}$ and $a^i = a^j$ iff $n$ divides $i - j$.

Proof. (i) Suppose $a$ has infinite order. Then there is no $n$ such that $a^n = e$.

(\Rightarrow) Assume $a^i = a^j$. Then $a^{i-j} = e$. So $a^{i-j} = a^0$. Thus $i - j = 0$ and $i = j$.

(\Leftarrow) If $i = j$, then $a^i = a^j$ follows directly.

(ii) Suppose $a$ has finite order $n$. Then $|a| = n$. Choose $x \in \{e, a, a^2, \ldots, a^{n-1}\}$. Then $x = a^k$ for some $k \in \mathbb{Z}$ so by definition, $x \in <a>$. Next choose $x \in <a>$. Then $x = a^k$ for some $k \in \mathbb{Z}$. By the division algorithm, $k = nq + r$ with $0 \leq r < n$. So

$$a^k = a^{nq+r} = a^n a^r = e a^r = a^r.$$  

Since $0 \leq r < n$ and $r \in \mathbb{Z}$, $x \in \{e, a, a^2, \ldots, a^{n-1}\}$. So, $<a> = \{e, a, a^2, \ldots, a^{n-1}\}$.

Now, we’ll show that $a^i = a^j$ iff $n$ divides $i - j$.

(\Rightarrow) Suppose $a^i = a^j$. Then $a^{j-i} = e = a^0$. By the division algorithm, $i-j = nq + r$ for $0 \leq r < n$. So

$$e = a^{j-i} = a^{nq+r} = a^n a^r = e a^r = a^r.$$  

This implies that $r = 0$, so $i-j = nq$, which is divisible by $n$.

(\Leftarrow) Suppose $n$ divides $i-j$. Then $i-j = nk$ for some $k \in \mathbb{Z}$. So $a^{i-j} = a^{nk} = e^k = e$. Thus, $a^{i-j} = e$ so $a^i = a^j$.

\qed

Corollary 3.5. For any group element $a$, $|a| = |<a>|$.

Corollary 3.6. Let $G$ be a group and let $a$ have order $n$. If $a^k = e$, then $n$ divides $k$.

Definition. If $H$ is a subgroup of $G$ and $a \in G$, then the left coset $aH$ is the subset

$$aH = \{ah : h \in H\}.$$

Example. $G = S_3 = \{(1), (1, 2), (1, 3), (1, 2, 3), (1, 3, 2), (2, 3)\}$ and $H = \{(1), (1, 2)\}$.

$$(1, 3)H = \{(1, 3), (1, 2, 3)\} \quad (2, 3)H = \{(2, 3), (1, 3, 2)\}.$$

Example. $G = \mathbb{Z}_{12} = \{0, 1, \ldots, 11\}$ and $H = \{0, 3, 6, 9\}$.

$$1 + H = \{1, 4, 7, 10\} \quad 2 + H = \{2, 5, 8, 11\}.$$

4. Cosets, Lagrange’s Theorem, and Normal Subgroups (by Lilith Ciccarelli)

Lemma 4.1. Let $H$ be a subgroup of $G$ with $a, b \in G$.

1. $aH = bH$ if and only if $b^{-1}a \in H$. In particular, $aH = H$ if and only if $a \in H$.
2. If $aH \cap bH \neq \emptyset$, then $aH = bH$.
3. $|aH| = |H|$ for all $a \in G$.

Proof. (1) (\Rightarrow) Assume $aH = bH$. Then $a \in bH$, which implies that $a = bh_0$ for some $H$.

\Rightarrow $b^{-1} = h_0$ \Rightarrow $b^{-1}a \in H$

(\Leftarrow) Assume $b^{-1} \in H$, which implies $b^{-1}a = h_0 \in H$ which then implies that $a = bh_0$ and $b = ah_0^{-1}$, since $H$ is a subgroup.

We want to show $aH = bH$. Begin by choosing $x \in aH$. Then $x = ah' = bh_0h'$. Since $h_0h' \in H$ (through closure), $x \in bH \leq aH$.

Now choose $y \in bH$. This implies that $y = bh' = ah_0^{-1} \in aH$, and thus $bH \leq aH$. Through containment, then $aH = bH$.

Now we prove that $aH = H$ if and only if $a \in H$.

(\Rightarrow) Let $aH = H = 1 \ast H$. Then $a^{-1} \in H$ and $a \in H$.

(\Leftarrow) Let $a \in H$. Then $1 \ast a \in H$, which implies that $aH = H$. 


Corollary 4.4. In a finite group $G$, the order of each element divides the order of the group. I.e. $|a| = |<a>|$.

Proof. Suppose $aH \cap bH \neq \emptyset$ then there exists an $x$ such that $x \in aH \cap bH$. $x = ah$ for some $h \in H = bh'$ for some $h' \in H$. Then $b^{-1}ah = h'$, so $b^{-1}a = h'h^{-1} \in H$. Now we know from part 1 that, since $b^{-1}a \in H, aH = bH$.

(3) To show that $|aH| = |H|$, define $f : H \to aH$ such that $f(h) = ah$ for each $h \in H$.

\[|G| = \sum_{i=1}^{t} |a_iH|\]

Since $|a_iH| = |H|, |G| = t|H|$. 
\[t = [G : H] \left[ \frac{|G|}{|H|} \right] \text{is called the index of H in G.} \]

\[\text{Corollary 4.3. If G is a finite group, and H is a subgroup of G, then [G : H] = \frac{|G|}{|H|}.}\]

\[\text{Corollary 4.4. In a finite group G, the order of each element divides the order of the group. I.e. |a| = |<a>|.}\]

\[\text{Corollary 4.5. A group of prime order is cyclic.}\]

Proof. Suppose $G$ has prime order $p$. Then let $a \in G$, with $a \neq e$. Then $|a|$ divides $|G|$. Since $a \neq e$, $|<a>| = 1$. Then $|<a>| = |G| = P$, since that’s the only other possibility. Thus, $G$ is generated by $a$.

Side note: $aH = Ha$ does not imply $ah = ha$. Instead, it means $ah = h'a$, where $h$ may or may not equal $h'$.

Definition. A subgroup $H$ of a group $G$ is called a normal subgroup of $G$ if $aH = Ha$ for all $a$ in $G$.

\[\text{Theorem 4.6 (Normal Subgroup Test). A subgroup H of G is a normal subgroup of G if and only if xHx^{-1} \subseteq H for all x \in G.}\]

Proof. $(\Rightarrow)$Let $H$ be a normal subgroup of $G$. Then $aH = Ha$. For $x \in G$, and $h \in H$, there is another element $h' \in H$ such that $xh = h'x$. This means $xhx^{-1} = h' \in H$ and thus, $xHx^{-1} \subseteq H$.

$(\Leftarrow)$ Let $xHx^{-1} \subseteq H$ for all $x$. Then for $x = a$, $aHa^{-1} \subseteq H, aH \subseteq Ha$ and $xH \subseteq Hx$. For $x = a^{-1}, a^{-1}H(a^{-1})^{-1} \subseteq H, Ha \subseteq aH$ and $Hx \subseteq xH$. This implies that $xH = Hx$ and therefore, $H$ is a normal subgroup.

\[\text{Example. Every subgroup of an abelian group is normal, since } ah = ha \text{ implies } aH = Ha.\]

\[\text{Example. The center } Z(G) \text{ is a normal subgroup, since for } h \in Z(G) \text{ and } a \in G, ah = ha \text{ implies } aH = Ha.\]

\[\text{Example. Let } A_n \text{ be the group of even permutations of } n. S_3 = \{(1), (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\} \]

\[A_3 = \{(1,2,3), (1,3,2), (1)\}\] (This is the alternating group of 3 elements) $(1,2)(1,2,3) = (1,3,2)(1,2) = (2,3)$

\[H = A_3 \text{ is a normal subgroup, since } ah = h'a \text{ for some } a \in G, h, h' \in H.\]

Definition. A Hamiltonian group is a group in which all its subgroups are normal.

5. Quotient Groups and Homomorphisms (by Linda Mummy)

Example. Dihedral Group

\[G = D_4 = \{r_0, r_{90}, r_{180}, r_{270}, h, v, d, d'\}\]

The cosets are

\[H = \{r_0, r_{180}\}\]

\[r_{90}H = \{r_{90}, r_{270}\}\]
There are no more cosets (recall that 2 cosets are either equal or their intersection is \( \emptyset \)).

Is \( H \) normal, i.e., \( H \triangleleft G \)? We need to check to see if \( gH = Hg \forall g \in G \). (Equivalently, \( xHx^{-1} \subseteq \forall x \in G \).)

We know \( xr_{180}x^{-1} = x^{-1}r_0 \in H \forall x \).

Now we only need to check that \( xr_{180}x^{-1} \subseteq H \forall x \in D_4 \).

**Theorem 5.1.** Let [\( G, \ast \)] be a group and \( H \triangleleft G \). Then the set of left cosets \( G/H = \{gH | g \in G \} \) forms a group under the operation \( (aH)(bH) = (a \ast b)H \).

**Proof.** Prove that the operation is well defined and has closure. Suppose \( aH = a'H \) and \( bH = b'H \) where \( a, a', b, b' \in G \). Then there exists \( h_1, h_2 \in H \) such that \( a' = ah_1 \) and \( b' = bh_2 \)

\[(a'H)(b'H) = (ah_1H)(bh_2H) = (aH)(bH)\]

There is closure. The identity is \( eH = H \). Inverses exist: \( (aH)^{-1} \). The elements are also associative:

\[(aH)(bH)cH = (abH)cH = abcH = aH(bcH) = aH(bH)(cH)\]

This is called the quotient group of \( G \) by \( H \) (aka the factor group of \( G \) by \( H \)). \( \square \)

**Example.** \( G = D_4, H = \{r_0, r_{180}\} = \{H, r_{90}H, vH, dH\} \)

**MULTIPLICATION TABLE for \( D_4 \)**

<table>
<thead>
<tr>
<th>( \circ )</th>
<th>( H )</th>
<th>( r_{90}H )</th>
<th>( vH )</th>
<th>( dH )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( H )</td>
<td>( H )</td>
<td>( r_{90}H )</td>
<td>( vH )</td>
<td>( dH )</td>
</tr>
<tr>
<td>( r_{90}H )</td>
<td>( r_{90}H )</td>
<td>( H )</td>
<td>( dH )</td>
<td>( vH )</td>
</tr>
<tr>
<td>( vH )</td>
<td>( vH )</td>
<td>( dH )</td>
<td>( H )</td>
<td>( r_{90}H )</td>
</tr>
<tr>
<td>( dH )</td>
<td>( dH )</td>
<td>( vH )</td>
<td>( r_{90}H )</td>
<td>( H )</td>
</tr>
</tbody>
</table>

**Example.** \( G = \mathbb{Z} \)

\( H = n\mathbb{Z} = \langle n \rangle = \{0, \pm n, \pm 2n, \ldots \} \).

\( H \) is normal because \( G \) is abelian. By the theorem, \( G/H \) exists. The elements of \( G/H \) are:

\[
0 + n\mathbb{Z} = \{0, 0 \pm n, \ldots \} \\
1 + n\mathbb{Z} = \{1, 1 \pm n, \ldots \} \\
2 + n\mathbb{Z} = \{2, 2 \pm n, \ldots \} \\
\vdots \\
n - 1 + n\mathbb{Z} = \{n - 1, n - 1 \pm n, \ldots \} \\
(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b) + n\mathbb{Z}
\]

Say \( n = 5 \). So \( G/H = \mathbb{Z}/(5\mathbb{Z}) \) and thus

\[
(1 + 5\mathbb{Z}) + (2 + 5\mathbb{Z}) = 3 + 5\mathbb{Z} \\
(2 + 5\mathbb{Z}) + (4 + 5\mathbb{Z}) = 1 + 5\mathbb{Z}
\]

This is just \( \mathbb{Z}_5 \) (and in general \( \mathbb{Z}_n \)).
QUESTION: What is the order of $G/H$? If $|G| < \infty$ then Lagrange’s Theorem implies

$$|G/H| = |G : H| = \frac{|G|}{|H|}.$$  

If $|G| = \infty$, anything is possible. For example,

$$|\mathbb{Z}/(n\mathbb{Z})| = n\text{ for } n > 0 \quad |\mathbb{Z}/0| = \infty$$

*Example.* The set of even permutations $A_4$ has no subgroup of order 6. $|A_4| = 12$ a subgroup of order 6 has index 2. If there exists a subgroup $H$ of order $G$, then $|G : H| = \frac{12}{6} = 2$ and so $H \triangleleft G$. Use this fact to check that $A_4$ does not in fact have such a subgroup.

**Definition.** Let $G, \hat{G}$ be groups. We say a mapping $\phi : G \to \hat{G}$ is a *homomorphism* if

$$\phi(gh) = \phi(g)\phi(h) \text{ for all } g, h \in G.$$  

We define the *kernel* of $\phi$ as

$$\ker \phi = \{ g \in G | \phi(g) \} = 1_{\hat{G}}$$

and the *image* of $\phi$ as

$$\text{im} \phi = \{ \phi(g) | g \in G \}.$$  

We say $\phi$ is an *isomorphism* if $\phi$ is 1-1 and onto (bijective).

Note: $\phi$ is 1-1 $\iff$ ker $\phi$ is trivial.

**Proof.** ($\Rightarrow$) If $\phi$ is 1-1 then $\phi(a) = \phi(b) \iff a = b$. Notice $\phi(1) = 1$ since

$$1_{\hat{G}} \cdot \phi(1) = \phi(1 \cdot 1) = \phi(1)\phi(1)$$

Thus $1_{\hat{G}}$ is the only thing that maps to $1_{\hat{G}}$ which implies that ker $\phi = 1_{\hat{G}}$.

($\Leftarrow$) Suppose $\phi(a) = \phi(b)$ for $a, b \in G$. Notice that $\phi(b^{-1}) = \phi(b)^{-1}$ as

$$\phi(b)\phi(b^{-1}) = \phi(b \cdot b^{-1}) = \phi(1) = 1.$$  

Multiply both sides of $\phi(a) = \phi(b)$ by $\phi(b^{-1})$ to get

$$\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(b)\phi(b^{-1}) = 1.$$  

However,

$$\ker \phi = \{ 1 \} \Rightarrow ab^{-1} = 1 \Rightarrow a = b. \quad \square$$

Note: $\phi$ is onto $\iff$ im $\phi = G$. (This follows directly from the definition of image)

**Examples.**

1. $\phi : \mathbb{Z} \to \mathbb{Z}_n$

   $$m \mapsto m \mod n \ (\phi(m) = m \mod n)$$

   $\phi$ is a homomorphism as it is well defined and $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in \mathbb{Z}$

2. $\phi : G \to G/H, \ H \triangleleft G$

   $$g \mapsto gH$$

   Is $\phi(ab) = \phi(a)\phi(b)$? Yes, by how we defined quotient groups.

3. $\phi : \mathbb{Z} \to \mathbb{Z}$

   $$x \mapsto x^2$$

   $\phi(a + b) = (a + b)^2$

   $\phi(a)\phi(b) = a^2 + b^2$

   Since $\phi(a + b) \neq \phi(a) + \phi(b)$, $\phi$ is not a homomorphism.
(4) $\phi : \mathbb{Z}_n \rightarrow \mathbb{Z}/(n\mathbb{Z})$

$$m \mapsto m + n\mathbb{Z}$$

This is a homomorphism (and an isomorphism!)

**Properties of Homomorphisms**

(1) $\phi(1_G) = 1_{\bar{G}}$

(2) $\phi(g^n) = (\phi(g))^n$ since $\phi(gg\ldots g)^n = \phi(g)\phi(g)\ldots\phi(g)$

(3) If $|g| < \infty$, $|\phi| = |g|

(4) $\ker \phi \leq G$

(5) If $H \leq G$, then $\phi(H) \leq \bar{G}$.

$$\phi(a)\phi(b^{-1}) = \phi(ab^{-1}) \subseteq \phi(H)$$ for all $a, b \in H$

(6) $H$ cyclic $\Rightarrow \phi(H)$ is cyclic

(7) $H$ abelian $\Rightarrow \phi(H)$ is abelian

(8) $H \triangleleft G$, then $\phi(H) \triangleleft \bar{G}$

(9) If $|H| = n$, then $|\phi(H)| | n$

**Theorem 5.2 (First Isomorphism Theorem).** Let $G, \bar{G}$ be groups and $\phi : G \rightarrow \bar{G}$ be an isomorphism. Then

$$\tau : G/\ker \phi \rightarrow \text{im} \phi$$

$$g \ker \phi \mapsto \phi(g)$$

is an isomorphism, written

$$G/\ker \phi \cong \text{im} \phi$$

**Proof.** $\tau$ is well defined. Let $H = \ker \phi$. Suppose $xH = yH$ for $x, y \in G$. We want to show that $\phi(x) = \phi(y)$, because we want $\tau(xH) = \tau(yH)$. We know $x^{-1}yH = H$. Therefore

$$x^{-1}y \in H = \ker \phi$$

$$\phi(x^{-1}y) = 1$$

$$\phi(x^{-1})\phi(y) = 1$$

$$\phi(y) = \phi(x)$$

$\tau$ is a homomorphism.

$$\tau(xy, H) = \phi(xy) = \phi(x)\phi(y) = \tau(xH)\tau(yH)$$

Is this map onto? Let $g' \in \text{im} \phi$. Then $g' = \phi(g)$ for some $g \in G$. Then $\tau(gH) = \phi(g) = g'$. Is $\tau$ 1-1? We want to show that $\tau(xH) = \tau(yH)$ then $xH = yH$. Suppose

$$\tau(xH) = \tau(yH) \Rightarrow \phi(x) = \phi(y)$$

$$\Rightarrow 1 = \phi(y)\phi(x^{-1}) = \phi(yx^{-1}).$$

$$\Rightarrow yx^{-1} \in \ker \phi = H$$

$$yx^{-1}H = H \Rightarrow yH = xH$$

$\Box$

**Definition.** For two groups $G, H$ define the external direct product of $G$ and $H$ as

$$G \oplus H = \{(g, h) | g \in G, h \in H\}$$

where the operations are componentwise.
6. Definition of a Ring (by Rob Davis)

Definition. A ring \( R \) is a set with two binary operations, addition \((a + b)\) and multiplication \((ab)\) such that for all \( a, b \in R \), the following hold:

1. \( a + b = b + a \)
2. \( a + (b + c) = (a + b) + c \)
3. There exists \( 0 \in R \) such that \( a + 0 = a \)
4. For every \( a \in R \), there exists \(-a\) such that \( a + (-a) = -a + a = 0 \)

These four properties tell us that \( R \) is an abelian group over addition. A ring further requires that

5. \( a(bc) = (ab)c \)
6. \( a(b + c) = ab + ac \) and \( (b + c)a = ba + ca \)

If \( ab = ba \), then \( R \) is a commutative ring. If \( R \) has an identity for multiplication, then it is a ring with unity. Further, a ring with unity does not necessarily have a multiplicative inverse for each element. Those elements that do have an inverse are called units.

Examples.

- \( \mathbb{Z} \) is a commutative ring with a unity element 1 and units \( \{1, -1\} \)
- \( \mathbb{R}, \mathbb{C}, \mathbb{Q} \) are commutative rings with unity and, and units are all nonzero elements of their respective sets
- \( \mathbb{Z}_n \) is a commutative ring with unity and units \( U(n) \)
- \( n\mathbb{Z} \) is a commutative ring and without unity for \( n > 1 \)
- \( GL(2, \mathbb{Z}) \) is a noncommutative ring with unity element
  \[
  \begin{pmatrix}
  1 & 0 \\
  0 & 1
  \end{pmatrix}
  \]
- \( GL(2, n\mathbb{Z}) \) is a noncommutative ring, and without unity for \( n > 1 \)
- \( GL(2, \mathbb{Z}_n) \) is a finite, noncommutative ring with unity
- \( R = \) the set of real-valued functions is a ring with unity \( f(x) = 1 \)

We again emphasize that rings do not necessarily have a multiplicative inverse for each element, therefore cancellation is not implied. That is,

\[ ab = ac \Rightarrow b = c \]

and

\[ a^2 = a \Rightarrow a = 0 \text{ or } a = 1. \]

If we do have the cancellation property, then \( R \) is an integral domain.

Rules of Multiplication:

1. \( a \cdot 0 = 0 \)
2. \( a(-b) = (-a)b = -ab \)
3. \( (-a)(-b) = ab \)
4. \( a(b - c) = ab - ac \) and \( (b - c)a = ba - ca \)
If $R$ has unity 1,

(5) $(-1)a = -a$

(6) $(-1)(-1) = 1$

**Partial Proof:**

(1) We see that $0 + a0 = a0 = a(0 + 0) = a0 + a0$, hence $0 + a0 = a0 + a0$. Subtracting $a0$ from both sides leaves us with $0 = a0$.

(2) Notice that $a(-b) + ab = a(-b + b) = a0 = 0$, so $a(-b) + ab = 0$. Subtracting $ab$ from both sides yields $a(-b) = ab$. A similar argument works to show $(-a)b = -ab$.

(3) The equations $0 = 0(-b) = (-a + a)(-b) = (-a)(-b) + a(-b)$ imply $0 = (-a)(-b) + a(-b)$. If we add $ab$ to each side, we see $ab = (-a)(-b) + a(-b) + ab = (-a)(-b)$. Therefore, $ab = (-a)(-b)$.

**Definition.** A subset $S$ of a ring $R$ is a subring of $R$ if $S$ is itself a ring with the operations on $R$.

**Theorem 6.1.** A nonempty subset $S$ of a ring $R$ is a subring if it is closed under subtraction and multiplication (Check to see if $a - b$ and $ab$ are in $S$ when $a, b \in S$).

**Examples.**

- $\{0\}, R$
- $R = \mathbb{Z}_6$ has unity 1, $S = \{0, 2, 4\}$ has unity 4
- $R = \mathbb{Z}_10$, $S = \{0, 2, 4, 6, 8\}$ has unity 6
- $R = \mathbb{Z}$, $S = n\mathbb{Z}$

Each of the following is a subring of the other: $6\mathbb{Z} \subset 3\mathbb{Z} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. We can also write $\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\} \subset \mathbb{C}$.

### 7. Integral Domains and Fields (by Sarah Behrens)

**Definition.** A zero-divisor is a nonzero element $a$ in a commutative ring $R$ such that there is a nonzero element $b$ with $ab = 0$.

**Definition.** An integral domain is a commutative ring with unity that has no zero-divisors. (A product equals zero only when one of the factors is zero.)

**Example.** $\mathbb{Z}, \mathbb{Z}[i], \mathbb{Z}_p (p$ is prime), $\mathbb{C}, \mathbb{R}, \mathbb{Q}$

**Note.** The existence of zero-divisors in a ring makes it hard to find zeros of polynomials whose coefficients are ring elements.

**Example.** $x^2 - 4x + 3 = 0$

Solve in $\mathbb{Z}$ and $\mathbb{Z}_{12}$.

$\mathbb{Z}$: $0 = x^2 - 4x + 3 = (x - 3)(x - 1)$. Thus $x = \{1, 3\}$.

$\mathbb{Z}_{12}$: (Method: check each element) $x = \{1, 3, 7, 9\}$.

**Theorem 7.1.** Let $a, b, c$ belong to an integral domain. If $a \neq 0$ and $ab = ac$, then $b = c$. (Cancellation Property)

**Proof.** $ab = ac$

$ab - ac = 0$

$a(b - c) = 0$

Since $a$ is not a zero-divisor:

$b - c = 0$

$b = c$
Definition. A field is a commutative ring with unity in which every nonzero element is a unit (has an inverse).

Note. (1) A field is a type of integral domain. (Let $a, b$ belong to a field $F$. Choose $a \neq 0$ with $ab = 0, a^{-1}ab = a^{-1}0, b = 0 \Rightarrow$ no zero divisors.) (2) A field is an algebraic system that is closed under $+, -, \cdot, \div$ (except 0).

Example. $C, \mathbb{R}, \mathbb{Q}, \mathbb{Z}_p$ ($p$ is prime).

Theorem 7.2. A finite integral domain is a field.

Proof. Let $D$ be a finite integral domain with unity 1. Let $a$ be any nonzero element of $D$. (Goal: show $a$ is a unit.) If $a = 1$, then $a$ is its own inverse, so we can assume that $a \neq 1$. Consider the sequence of elements $a, a^2, a^3, \cdots$. Since $D$ is finite, there must be $a_i = a_j$ for some $i > j$.

$$a_i = a^j$$
$$a^{j+k} - a^j = 0$$
$$a^j(a^k - 1) = 0$$
$$\Rightarrow a^k - 1 = 0$$
$$a^k = 1$$

But since $a \neq 1$
$$\Rightarrow k > 1$$
$$aa^{k-1} = 1$$
$$\Rightarrow a^{-1} = a^{k-1} \square$$

Corollary 7.3. $\mathbb{Z}_p$ is a field.

Proof. Suppose $a, b \in \mathbb{Z}_p$ and $ab = 0$. Then $ab = pk$ for some $k$. By Euclid’s Lemma (below) $p$ divides $a$ or $p$ divides $b$ so either $a = pm$ or $b = pn$ in $\mathbb{Z}_p$. Hence $a = 0$ or $b = 0$ and $a, b$ are not zero-divisors. Thus $\mathbb{Z}_p$ is an integral domain. By the previous theorem, $\mathbb{Z}_p$ is a field. \square

Lemma 7.4 (Euclid’s Lemma). If $p$ is a prime and $p$ divides $ab$, then $p$ divides $a$ or $p$ divides $b$.

Example. (Another finite field example)
$\mathbb{Z}_3[i] = \{a + bi : a, b \in \mathbb{Z}_3\} = \{0, 1, 2, i, 2i, 1 + i, 1 + 2i, 2 + i, 2 + 2i\}$
$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : ab \in \mathbb{Q}\}$

Definition. The characteristic of a ring $R$ is the least positive integer $n$ such that $nx = 0 \ \forall x \in R$

- If no such integer exists we say $R$ has characteristic zero.
- We denote the characteristic by char $R$.

Example. $\mathbb{Z}_3[i]$, char $\mathbb{Z}_3[i] = 3 \ x + x + x = 0$
$\mathbb{Z}_n$ has characteristic $n$
$\{0, 3, 6, 9\}_{12}$ has characteristic 4

Theorem 7.5. Let $R$ be a ring with unity 1.

- If 1 has infinite order under addition, then char $R = 0$.
- If 1 has order $n$ under addition, then char $R = n$.

Proof. • If 1 has infinite order, then there is no $n$ such that $n \cdot 1 = 0$, so $R$ has characteristic 0.
• If 1 has order \( n \), then \( n \cdot 1 = 0 \) and \( n \) is the least such \( n \) with this property. But for \( x \),
\[
n \cdot x = x + x + \cdots + x
\]
\[
= 1x + 1x + \cdots + 1x
\]
\[
= (1 + 1 + \cdots + 1) \cdot x
\]
\[
= (n \cdot 1) \cdot x
\]
\[
= 0 \cdot x
\]
\[
= 0
\]
Thus \( R \) has characteristic \( n \).

8. Ideals and Factor Rings (by Annette Honken)

Definition. A subring \( A \) of a ring \( R \) is called an ideal of \( R \) if for every \( r \in R \) and \( a \in A \), \( ar \in A \) and \( ra \in A \).

\[
rA = \{ ra | a \in A \} \subset A \quad \text{ (left ideal)}
\]
\[
Ar = \{ ar | a \in A \} \subset A \quad \text{ (right ideal)}
\]

Theorem 8.1. A nonempty subset \( A \) of a ring \( R \) is an ideal of \( R \) if
(1) \( a - b \in A \) whenever \( a, b \in A \)
(2) \( ra \) and \( ar \) are in \( A \) whenever \( a \in A \) and \( r \in R \)

Examples of Ideals:
(1) \( R \) and \( \{0\} \) are ideals of \( R \)
(2) \( R = \mathbb{Z} \) and \( n\mathbb{Z} = \{ 0, \pm n, \pm 2n, \ldots \} \) is an ideal of \( \mathbb{Z} \)

Definition. Let \( R \) be a commutative ring with unity and let \( a \in R \). The set \( < a > = \{ ra | r \in R \} \) is an ideal of \( R \) called the principal ideal generated by \( a \).

Example. \( (1) \) \( R[x] \) = ring of polynomials with real coefficients. \( A = \langle x \rangle = \{ \) set of polynomials with \( a_0 = 0 \} \) (\( A \) is an ideal of \( R[x] \)).
\( (2) \) \( I \) = \( \langle a_1, a_2, \ldots, a_n \rangle = \{ r_1a_1 + r_2a_2 + \ldots + r_na_n \} \)

Definition. Since \( R \) is a group under addition and \( A \) is a normal subgroup of \( R \), we can form the factor ring \( R/A = \{ r + A | r \in R \} \).

Theorem 8.2. Existence of Factor Rings - Let \( R \) be a ring and let \( A \) be a subring of \( R \). The set of cosets \( \{ r + A | r \in R \} \) is a factor ring under the operations \( (s + A) + (t + A) = (s + t) + A \) and \( (s + A)(t + A) = st + A \) if and only if \( A \) is an ideal of \( R \).

Proof. \( \{ r + A \} \) forms a group under addition. (Assoc. and dist. are trivial). Check: Multiplication is a binary operation. Show \( A \) is an ideal if and only if multiplication is well-defined.

(\( \Rightarrow \)) \( A \) is an ideal. Let \( s + A = s' + A \) and \( t + A = t' + A \). Since \( A \) is an ideal, \( s = s' + a \) and \( t = t' + b \) for \( a, b \in A \).
\[
st = (s' + a)(t' + b) = s't' + at' + s'b + ab
\]
\[
st + A = s't' + at' + s'b + ab + A = s't' + A
\]
Coset multiplication is well-defined.

(\( \Leftarrow \)) Now, show well-defined implies \( A \) is an ideal. We will show the contrapositive. Thus, we will show that \( A \) not an ideal implies that it is not well-defined. Suppose \( A \) is a subring that is not an ideal. Then, there exists \( a \in A \) and \( r \in R \) such that \( ar \notin A \) (or \( ra \notin A \)). Assume it is \( ar \) that is not in \( A \). Consider \( a + A = 0 + A \) and \( r + A \). We see that \( (a + A)(r + A) = ar + A \), but \( (0 + A)(r + A) = 0 + A = A \). We note that \( ar + A \neq A \). Then, multiplication is not well-defined, which implies that the set of cosets is not a ring.

Examples.
\[ \mathbb{Z}/4\mathbb{Z} = \{ 0 + 4\mathbb{Z}, 1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}, 3 + 4\mathbb{Z} \} \]
\[ 2\mathbb{Z}/6\mathbb{Z} = \{ 0 + 6\mathbb{Z}, 2 + 6\mathbb{Z}, 4 + 6\mathbb{Z} \} \]
\[ R = \left\{ \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} | a_i \in \mathbb{Z} \right\}, \quad I = \left\{ \begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix} | b_i \in 2\mathbb{Z} \right\}, \quad R/I = \left\{ \begin{bmatrix} c_1 & c_2 \\ c_3 & c_4 \end{bmatrix} + I | c_i \in \{0, 1\} \right\} \]
• $\mathbb{R}[x]$ = ring of polynomials with real coefficients. $< x^2 + 1 >$ = principal ideal generated by $x^2 + 1 = \{f(x)(x^2+1)|f(x) \in \mathbb{R}[x]\}$. Then, $\mathbb{R}[x]/< x^2 + 1 >$ = \{\(g(x) + < x^2 + 1 > | g(x) \in \mathbb{R}[x]\)\} = \{ax + b + < x^2 + 1 > | a, b \in \mathbb{R}\}. g(x) = q(x)(x^2+1) + r(x)$ by division algorithm - degree of $r(x) < 2 \Rightarrow r(x) = ax + b, g(x) + < x^2 + 1 > = g(x)(x^2+1) + r(x) + < x^2 + 1 > = r(x) + < x^2 + 1 > = ax + b + < x^2 + 1 >$.

• $R = \mathbb{Z}[i]/< 2-i >$ Elements have the form $a+bi < 2-i >$. Since $2-i+ < 2-i > = 0 + < 2-i >$, $2-i = 0 \Rightarrow i = 2 \Rightarrow i^2 = -1 = 4 \Rightarrow -1 = 4 \Rightarrow 0 = 5$.

**Definition.** A prime ideal of a commutative ring $R$ is a proper ideal of $R$ such that $a, b \in R$ and $ab \in A$ imply $a \in A$ or $b \in A$.

**Example.** $R = \mathbb{Z}, I = 5\mathbb{Z}, I = 6\mathbb{Z}$

**Definition.** A maximal ideal $A$ of a commutative ring $R$ is a proper ideal of $R$ such that whenever $B$ is an ideal of $R$ containing $A$, $A \subseteq B \subseteq R$, then either $A = B$ or $B = R$. (Can’t have $A \subset B \subset R$).

**Theorem 8.3.** Let $R$ be a commutative ring with unity with $A$ an ideal of $R$. $R/A$ is an integral domain if and only if $A$ is prime.

**Proof.** ($\Rightarrow$) Suppose $R/A$ is an integral domain. Let $ab \in A$. Then, $(a+A)(b+A) = ab + A = A$. Since $R/A$ is an integral domain, either $a + A = A$ or $b + A = A$, so either $a \in A$ or $b \in A$. Therefore, $A$ is prime.

($\Leftarrow$) Know $R/A$ is a commutative ring with unity. Our goal is to show that when $A$ is prime, $R/A$ has no zero divisors. Let $A$ be prime. $(ab \in A \Rightarrow a \in A$ or $b \in A)$. Let $(a+A)(b+A) = A$ (want either $a + A = A$ or $b + A = A$). $\Rightarrow ab + A = A \Rightarrow ab \in A$ Since $A$ is prime, $a \in A$ or $b \in A$. ($a + A = A$ or $b + A = A$). So, $R/A$ is an integral domain.

**Theorem 8.4.** Let $R$ be a commutative ring with unity with $A$ an ideal of $R$. $R/A$ is a field if and only if $A$ is maximal.

**Proof.** ($\Rightarrow$) Suppose $R/A$ is a field. let $B$ be an ideal that properly contains $A$. $A \subset B \subset R$ Choose $b \in B$ such that $b \notin A$. Then, $b + A \neq 0 + A$. Since $R/A$ is field, there exists $c + A$ such that $(b + A)(c + A) = 1 + A \Rightarrow bc + A = 1 + A \Rightarrow 1 - bc \in A$. $1 = (1 - bc) + bc \in B$ so $B = R$ and $A$ is maximal.

($\Leftarrow$) Suppose $A$ is maximal. Let $b \in R$, but $b \notin A$. Show $b + A$ has an inverse. $B = \{br + A|r \in R, a \in A\}$. This $B$ is an ideal that properly contains $A$. $A \subset B \subset R$ Since $A$ is maximal, $B = R$. Then, $1 \in B$ and $1 = bc + a’$. $1 + A = bc + a’ + A = bc + A = (b + A)(c + A)$, so $(b + A)$ has an inverse and $R/A$ is a field.

9. Ring Homomorphisms (by Nathan McNew)

**Definition.** A ring homomorphism $\phi$ from a ring $R$ to a ring $S$ is a mapping that preserves ring operations. Specifically, for all $a, b \in R$,

$$\phi(a + b) = \phi(a) + \phi(b)$$

$$\phi(ab) = \phi(a)\phi(b)$$

A ring homomorphism that is both 1-1 and onto is a ring isomorphism.

**Examples.**

- $\phi: \mathbb{Z} \rightarrow \mathbb{Z}_n, \phi(k) = k \mod n$
- $\phi: \mathbb{C} \rightarrow \mathbb{C}, \phi(a + bi) = a - bi$
- $\phi: \mathbb{R}[x] \rightarrow R, \phi(f(x)) = f(1)$
- $\phi: \mathbb{Z}_4 \rightarrow \mathbb{Z}_{10}, \phi(x) = 5x$

**Proof.** Let $x, y \in \mathbb{Z}$. By the division algorithm let $x + y = 4q_1 + r_1$ and $xy = 4q_2 + r_2$. Then we can write $r_1 = x + y - 4q_1$ and $r_2 = xy - 4q_2$. Then working first within $\mathbb{Z}_4$ we have

$$\phi(x + y) = \phi(r_1) = 5(x + y - 4q_1)$$

$$= 5x + 5y - 20q_1$$

$$= 5x + 5y \ (\text{in } \mathbb{Z}_{10})$$

$$= \phi(x) + \phi(y)$$
and

\[ \phi(xy) = \phi(r_2) = 5(xy - 4q_2) \]
\[ = 5xy - 20q_1 \]
\[ = 25xy \text{ (in } \mathbb{Z}_{10}) \]
\[ = (5x)(5y) \]
\[ = \phi(x)\phi(y) \]

\[ \square \]

**Note.** Group isomorphic sets are not necessarily ring isomorphic. Take for example \( \mathbb{Z} \) and \( 2\mathbb{Z} \).

**PROPERTIES OF RINGS**

**Theorem 9.1.** Let \( \phi \) be a ring homomorphism from a ring \( R \) into a ring \( S \). Let \( A \) be a subring of \( R \) and let \( B \) be an ideal of \( S \).

1. For any \( r \in R \) and positive integer \( n \), \( \phi(nr) = n\phi(r) \) and \( \phi(r^n) = \phi(r)^n \).
2. \( \phi(A) = \{ \phi(a) | a \in A \} \) is a subring of \( S \).
3. If \( A \) is an ideal and \( \phi \) is onto then \( \phi(A) \) is an ideal.
4. \( \phi^{-1}(B) \) is an ideal in \( R \).
5. If \( R \) is commutative then \( \phi(R) \) is commutative.
6. If \( R \) has unity \( 1 \), \( S \neq \{ 0 \} \) and \( \phi \) is onto then \( \phi(1) \) is the unity.
7. \( \phi \) is an isomorphism if and only if \( \phi \) is onto and \( \ker \phi = 0 \).
8. If \( \phi \) is an isomorphism then \( \phi^{-1} \) is an isomorphism.

**Theorem 9.2.** Let \( \phi \) be a ring homomorphism from a ring \( R \) to a ring \( S \). Then \( \ker \phi \) is an ideal of \( R \).

**Proof.** Let \( a, b \in \ker \phi \), \( r \in R \). then consider \( \phi(a - b) = \phi(a) + \phi(-b) = \phi(a) - \phi(b) = 0 - 0 = 0 \). Thus \( a - b \in \ker \phi \). Also, \( \phi(ra) = \phi(r)\phi(a) = \phi(r)0 = 0 \), so \( ra \in \ker \phi \). Thus \( \ker \phi \) is an ideal. \( \square \)

**Theorem 9.3** (First Isomorphism Theorem for Rings). Let \( \phi \) be a ring homomorphism from \( R \) to \( S \). Then the mapping from \( R/ \ker \phi \) to \( \phi(R) \) given \( b r + \ker \phi \rightarrow \phi(r) \) is an isomorphism. \((R/ \ker \phi \cong \phi(R)) \)

**THE FIELD OF QUOTIENTS**

Recall \( \mathbb{Z} \) is not a field, but \( \mathbb{Q} \) is.

**Theorem 9.4.** Let \( D \) be an integral domain. Then there exists a field \( F \) called the field of quotients of \( D \) that contains a subring isomorphic to \( D \).

**Proof.** Let \( S = \{(a, b) | a, b \in D, b \neq 0 \} \) Define an equivalence relation on \( S \) by \((a, b) \equiv (c, d) \) if \( ad = bc \). Let \( F \) be the set of equivalence classes of \( S \) under the relation \( \equiv \) and denote the equivalence class containing \((x, y) \) by \( \frac{a}{b} \). Define addition and multiplication by

\[ \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \]
\[ \left( \frac{a}{b} \right) \left( \frac{c}{d} \right) = \frac{ac}{bd} \]

We now show that these relations are well-defined on \( F \). Let \( \frac{a}{b} = \frac{a'}{b'} \) and \( \frac{c}{d} = \frac{c'}{d'} \).

**Addition:** (Want to show \( \frac{ad + bc}{bd} = \frac{a'd' + b'c'}{a'd' + b'c'} \))

\[ (ad + bc)b'd' = adb'd' + bcb'd' \]
\[ = ab'd'd' + cd'bb' \]
\[ = a'b'd'd' + c'ddb' \]
\[ = a'd'bd + b'c'bd \]
\[ = (a'd' + b'c')bd \]
Multiplication: 

\( \text{Want to show } \frac{ac}{bd} = \frac{a'c'}{b'd'} \)

\[ acb'd' = ab'cd' \]

\[ = ba'dc' \]

\[ = bd(a'c') \]

For \( F \) to be a field, let 1 be the unity element for \( D \). Then \( 0 \neq 1 \) is the additive identity for \( F \), is the multiplicative identity, \( \frac{c}{a} \) is the additive inverse and \( \frac{c}{a} \) is the multiplicative inverse.

\( \square \)

Example. \( D = \mathbb{Z}[x], F = \{ \frac{f(x)}{g(x)} | f(x), g(x) \in D, g(x) \neq 0 \} \)

10. Polynomial Rings (by Nathan Salazar)

Definition. Let \( R \) be a commutative ring. \( R[x] = \{ a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 | a_i \in R, \ n \text{ is a non-negative integer} \} \) is called the ring of polynomials over \( R \) in the indeterminate \( x \). Two elements \( a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 \) and \( b_mx^m + b_{m-1}x^{m-1} + \ldots + b_1x + b_0 \) are equal if \( a_i = b_i \forall i \).

- In \( \mathbb{Z}_3[x] \), if \( f(x) = x^3 \) and \( g(x) = x^5 \), then \( f(x) \neq g(x) \), even though, in \( \mathbb{Z}_3, f(0) = 0 = g(0) \), \( f(1) = 1 = g(1) \), and \( f(2) = 2 = g(2) \).
- In \( \mathbb{Z}_3[x] \), let \( f(x) = 2x^3 + x^2 + 2x + 2 \) and \( g(x) = 2x^2 + 2x + 1 \). Then \( f(x) + g(x) = 2x^3 + x, \) and \( f(x)g(x) = x^5 + 2x^3 + 2 \).

Division Algorithm

Let \( F \) be a field and let \( f(x), g(x) \in F[x] \), with \( g(x) \neq 0 \). Then there exist unique polynomials \( q(x) \) and \( r(x) \) in \( F[x] \) such that \( f(x) = g(x)q(x) + r(x) \), with either \( r(x) = 0 \) or \( \deg(r(x)) < \deg(g(x)) \).

Example. Let \( f(x) = 3x^4 + x^3 + 2x^2 + 1 \) and let \( g(x) = x^2 + 4x + 2 \) in \( \mathbb{Z}_5[x] \). Then \( f(x) \div g(x) = \)

\[
\begin{array}{c|cccc}
3x^2 + 4x & 3x^4 + x^3 + 2x^2 + 0x + 1 \\
+ (3x^4 + 2x^3 + x^2) & -4x^3 + x^2 + 0x + 1 \\
- (4x^3 + x^2 + 3x) & -0x^2 + 2x + 1 \\
\end{array}
\]

Thus, we can write \( f(x) = (x^2 + 4x + 2)(3x^2 + 4x) + (2x + 1) \).

Theorem 10.1. If \( D \) is an integral domain, then \( D[x] \) is an integral domain.

Proof. We know \( D[x] \) is a ring, because \( D \) is a ring. Also, if \( D \) is commutative, then \( D[x] \) is commutative, and \( f(x) = 1 \) is the multiplicative identity. Now, suppose \( f(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 \) and \( g(x) = b_mx^m + b_{m-1}x^{m-1} + \ldots + b_1x + b_0 \), where \( a_n \neq 0 \) and \( b_m \neq 0 \). Then \( f(x)g(x) \) has leading coefficient \( a_nb_m \neq 0 \), since \( D \) is an integral domain. Therefore, the product of two non-zero polynomials cannot give 0, and so \( D[x] \) is an integral domain.

\( \square \)

Theorem 10.2 (The Remainder Theorem). Let \( F \) be a field with \( a \in F \) and \( f(x) \in F[x] \). Then \( f(a) \) is the remainder when \( f(x) \) is divided by \( x - a \).

Theorem 10.3 (The Factor Theorem). Let \( F \) be a field, \( a \in F, \) and \( f(x) \in F[x] \). Then \( a \) is a zero of \( f(x) \) if and only if \( x - a \) is a factor of \( f(x) \).

Definition. A principle ideal domain is an integral domain \( R \) in which every ideal has the form \( \langle a \rangle = \{ ra | r \in R \} \) for some \( a \in R \).

Theorem 10.4. Let \( F \) be a field. Then \( F[x] \) is a principal ideal domain.
Proof. We already know that \( F[x] \) is an integral domain. Let \( I \) be an ideal in \( F[x] \). If \( I = \{0\} \), then 
\[ I = \langle 0 \rangle. \]
If \( I \neq \{0\} \), then choose an element \( g(x) \in I \), where \( g(x) \) has minimum degree in \( I \), and \( g(x) \neq 0 \).
We want to show that \( I = \langle g(x) \rangle \). We know \( \langle g(x) \rangle \subseteq I \).
We show that \( I \subseteq \langle g(x) \rangle \).
Choose \( f(x) \in I \).
Using the division algorithm, \( f(x) = q(x)g(x) + r(x) \), with either \( r(x) = 0 \) or \( \deg(r(x)) < \deg(g(x)) \).
Now, \( r(x) = f(x) - g(x)g(x) \in I \). Since \( g(x) \) is an element of minimal degree, and \( \deg(r(x)) < \deg(g(x)) \), we must have \( r(x) = 0 \).
Therefore \( f(x) \in \langle g(x) \rangle \), and so \( I \subseteq \langle g(x) \rangle \).

\[ \square \]

11. Polynomial Factorization (by Lisa Moats)

Definition. Let \( D \) be an integral domain. A polynomial \( f(x) \in D[x] \) that is neither the zero polynomial nor
a unit in \( D[x] \) is said to be irreducible over \( D \), if, whenever \( f(x) \) is expressed as the product \( f(x) = g(x)h(x) \),
with \( g(x), h(x) \in D[x] \), then \( g(x) \) or \( h(x) \) is a unit in \( D[x] \).
A nonzero, nonunit element of \( D[x] \) that is not irreducible over \( D \) is called reducible.

Example. \( f(x) = 2x^2 + 4 = 2(x^2 + 2) \) is irreducible over \( \mathbb{Q} \) and \( \mathbb{R} \). However, it is reducible over \( \mathbb{Z} \) since \( 2 \) and \( x^2 + 2 \) are not units in \( \mathbb{Z} \).
In \( \mathbb{C} \), \( f(x) = 2x^2 + 4 = 2(x + i\sqrt{2})(x - i\sqrt{2}) \) is reducible over \( \mathbb{C} \).

Definition. When the integral domain is a field, \( f(x) \in F[x] \) is irreducible if \( f(x) \) cannot be written as a product of two polynomials of lower degree.

Example. \( f(x) = x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2}) \) is reducible over \( \mathbb{R} \) but not over \( \mathbb{Q} \).

Theorem 11.1. Let \( F \) be a field. If \( f(x) \in F[x] \) and \( \deg f(x) \) is 2 or 3, then \( f(x) \) is reducible over \( F \) if
and only if \( f(x) \) has a zero in \( F \).

Proof. \((\Rightarrow)\) Let \( f(x) = g(x)h(x) \) where both \( g(x) \) and \( h(x) \) are in \( F[x] \), and have degree less than that of \( f(x) \).
Then, since \( \deg f(x) = \deg g(x) + \deg h(x) \) and \( \deg f(x) = 2 \) or 3, then at least one of \( g(x) \) or \( h(x) \)
has degree 1. Without loss of generality, assume \( \deg g(x) = 1 \). Then, \( g(x) = ax + b \) for some \( a, b \in F \).
Since \( F \) is a field, \( a^{-1} \in F \), so \( -a^{-1}b \in F \). Then, \( g(-a^{-1}b) = a(-a^{-1}b) + b = 0 \) so \( -a^{-1}b \) is a zero of \( g(x) \).
Thus, \( -a^{-1}b \) is a zero of \( f(x) \).

\((\Leftarrow)\) Suppose \( f(a) = 0 \) where \( a \in F \). Then \( x - a \) is a factor of \( f(x) \). Therefore, \( f(x) \) is reducible, since
\( f(x) = (x - a)h(x) \) where \( h(x) \in F[x] \).

Example. In \( \mathbb{Z}_5 \), \( f(x) = x^2 + 1 \) is reducible since \( f(2) = 0 \).
In \( \mathbb{Z}_3 \), \( f(x) = x^2 + 1 \) is irreducible since \( f(0) = 1, f(1) = 2, \) and \( f(2) = 2 \).

Note. Sometimes a polynomial with degree greater than 3 may be reducible over a field, but have no zeros in the field. For example, \( f(x) = x^4 + 2x^2 + 1 = (x^2 + 1)^2 \) is reducible over \( \mathbb{R} \) but has no zeros in \( \mathbb{R} \).

Definition. The content of a nonzero polynomial \( a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 \), where \( a_i \in \mathbb{Z} \) for each
\( i \) with \( 1 \leq i \leq n \), is the greatest common divisor of the integers \( a_n, a_{n-1}, \ldots, a_1, a_0 \).

Definition. A primitive polynomial is an element of \( \mathbb{Z}[x] \) with content 1.

Theorem 11.2 (Gauss’ Lemma). The product of two primitive polynomials is primitive.

Proof. Let \( f(x) \) and \( g(x) \) be primitive. Suppose \( f(x)g(x) \) is not primitive. Let \( p \) be a prime divisor of the content of \( f(x)g(x) \). Let \( f(x), g(x) \) be the polynomials obtained from reducing the coefficients of \( f(x), g(x) \) and \( f(x)g(x) \) mod \( p \), respectively. Then, \( f(x), g(x) \in \mathbb{Z}_p[x] \), and \( f(x)g(x) \) = 0 by how \( p \) was defined. Recall \( \mathbb{Z}_p[x] \) is an integral domain. So \( f(x)g(x) = f(x)g(x) = 0 \). Then either \( f(x) = 0 \) or \( g(x) = 0 \).
This means that \( p \) either divides every coefficient of \( f(x) \) or of \( g(x) \). So, either \( f(x) \) is not primitive or \( g(x) \)
is not primitive. This is a contradiction. Therefore, \( f(x)g(x) \) must be primitive.

Theorem 11.3. Let \( f(x) \in \mathbb{Z}[x] \). If \( f(x) \) is reducible over \( \mathbb{Q} \), then \( f(x) \) is reducible over \( \mathbb{Z} \).
Irreducibility Tests.

**Theorem 11.4.** Let \( p \) be a prime and suppose \( f(x) \in \mathbb{Z}[x] \) with \( \deg f(x) \geq 1 \). Let \( \overline{f}(x) \) be the polynomial in \( \mathbb{Z}_p[x] \) obtained from \( f(x) \) by reducing all the coefficients of \( f(x) \mod p \). If \( \overline{f}(x) \) is irreducible over \( \mathbb{Z}_p[x] \) and \( \deg \overline{f}(x) = \deg f(x) \), then \( f(x) \) is irreducible over \( \mathbb{Q} \).

**Example.** Let \( f(x) = 21x^3 - 3x^2 + 2x + 9 \). Over \( \mathbb{Z}_2 \), \( \overline{f}(x) = x^3 - x^2 + 1 \). Notice \( \overline{f}(0) = 1, \overline{f}(1) = 1 \), and \( \deg \overline{f}(x) = \deg f(x) = 3 \). Thus, by reducibility in degrees 2 and 3, \( f(x) \) is irreducible over \( \mathbb{Z}_2 \). So by the mod \( p \) theorem, \( f(x) \) is irreducible over \( \mathbb{Q} \).

**Theorem 11.5 (Eisenstein’s Criterion).** Let \( f(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 \in \mathbb{Z}[x] \). If there is a prime \( p \) such that \( p \not| a_n, p|a_{n-1}, \ldots, p|a_0 \) and \( p^2 \not| a_0 \), then \( f(x) \) is irreducible over \( \mathbb{Q} \).

12. Extension Fields (by Robert Arn)

Show \( \mathbb{R}[x]/\langle x^2 + 1 \rangle \cong \mathbb{C} \phi : \mathbb{R}[x] \to \mathbb{C} \) by \( \phi(f(x)) = f(c) \). Then \( x^2 + 1 \in \ker \phi \). \( x^2 + 1 \) is a polynomial of minimum degree in \( \ker \phi \). Then \( \ker \phi = \langle x^2 + 1 \rangle \). By 1st isomorphism \( \mathbb{R}[x]/\langle x^2 + 1 \rangle \cong \mathbb{C} \).

There is a connection among irreducible polynomials, maximal ideals, and fields.

**Theorem 12.1.** Let \( F \) be a field and let \( p(x) \in F[x] \). Then \( \langle p(x) \rangle \) is a maximal ideal in \( F[x] \) if and only if \( p(x) \) is irreducible over \( F \).

**Proof.** \( \Rightarrow \) Suppose \( \langle p(x) \rangle \) is a maximal ideal in \( F[x] \). Then \( p(x) \) is neither the zero polynomial nor an unit in \( F[x] \). If \( p(x) = g(x)h(x) \) (a factorization of lower degree). Then \( \langle p(x) \rangle \not\subseteq \langle g(x) \rangle \subseteq F[x] \). So either \( \langle g(x) \rangle = \langle p(x) \rangle \) or \( \langle g(x) \rangle = F[x] \). If \( \langle g(x) \rangle = \langle p(x) \rangle \), the degree \( g(x) = \deg p(x) \). If \( \langle g(x) \rangle = F[x] \) then \( \deg g(x) = 0 \) and \( \deg p(x) = \deg h(x) \). So \( p(x) \) cannot be written as the product of lower degree.

\( \Leftarrow \) Now, suppose \( p(x) \) is irreducible over \( F \). Let \( I \) be an ideal of \( F[x] \) such that \( \langle p(x) \rangle \subseteq I \subseteq F[x] \). Since \( F[x] \) is a principle ideal domain, \( I = \langle g(x) \rangle \) for some \( g(x) \in F[x] \). So \( p(x) \in \langle g(x) \rangle \Rightarrow p(x) = g(x)h(x) \) where \( h(x) \in F[x] \). Since \( p(x) \) is irreducible either \( g(x) \) or \( h(x) \) is constant. If \( g(x) \) is constant, \( \langle g(x) \rangle = I = F[x] \). If \( h(x) \) is constant, \( \langle p(x) \rangle = \langle g(x) \rangle \). So \( \langle p(x) \rangle \) is maximal.

**Corollary 12.2.** Let \( G \) be a field and \( p(x) \) an irreducible over \( F \). Then \( F[x]/\langle p(x) \rangle \) is a field.

**Definition.** An integral domain \( D \) is a **Unique Factorization Domain (UFD)** if

1. Every nonzero element of \( D \) that is not a unit can be written as a product of irreducible of \( D \), and
2. The factorization into irreducible is unique up to isomorphism up to associates and the order in which the factors appear.

For \( F \) a field, \( F[x] \) is a UFD.

**Definition.** A field \( E \) is an extension field of a field \( F \) is \( F \subseteq E \) and the operations of \( F \) are those of \( E \) restricted to \( F \).

**Theorem 12.3 (Fundamental Theorem of Field Theory (Kronecker’s Theorem)).** Let \( F \) be a field and \( f(x) \) a nonconstant polynomial in \( F[x] \). Then there is an extension field \( E \) of \( F \) in which \( f(x) \) has a zero.

**Proof.** Since \( F[x] \) is a UFD, \( f(x) \) has an irreducible factor, say \( p(x) \). We can construct an extension field \( E \) of \( F \) in which \( p(x) \) has a zero. Consider \( F[x]/\langle p(x) \rangle = E \). From our first theorem, \( F[x]/\langle p(x) \rangle \) is a field. The mapping \( \phi : F \to E \) given by \( \phi(a) = a + \langle p(x) \rangle \). \( \phi \) is a \( 1-1 \) homomorphism (Think of \( E \) as containing \( F \) as a equal to \( a + \langle p(x) \rangle \)). Now, show \( p(x) \) has a zero in \( E \). \( p(x) = a_nx^n + \ldots + a_0 \). In \( E \), \( x + \langle p(x) \rangle \) is a zero of \( p(x) \).

\[
p(x + \langle p(x) \rangle) = a_n(x + \langle p(x) \rangle)^n + a_{n-1}(x + \langle p(x) \rangle)^{n-1} + \ldots + a_0
= a_n(x^n + \langle p(x) \rangle) + \ldots + a_0
= a_nx^n + a_{n-1}x^{n-1} + \ldots + a_0 + \langle p(x) \rangle
= p(x) + \langle p(x) \rangle
= \langle p(x) \rangle
= 0 + \langle p(x) \rangle
\]
Examples. (1) Let \( f(x) = x^2 + 1 \in \mathbb{Q}[x] \) \( F = \mathbb{Q} \) \( \phi : F \to E \phi : a \to a + \langle p(x) \rangle \)
\[
\phi(x) = x + (x^2 + 1) \\
E = \mathbb{Q}[x]/(x^2 + 1) \\
x \to x + (x^2 + 1) \\
f(x) \to f(x + (x^2 + 1)) \\
(x + (x^2 + 1))^2 + 1 = x^2 + (x^2 + 1) + 1 = x^2 + 1 + (x^2 + 1) = \langle x^2 + 1 \rangle
\]
(2) Let \( f(x) = x^5 + 2x^2 + 2x + 2 \in \mathbb{Z}_3 = \langle x^2 + 1 \rangle \langle x^3 + 2x + 2 \rangle \) \( E = \mathbb{Z}[x]/(x^2 + 1) = \{ (x^2 + 1), 1 + (x^2 + 1), 2 + \langle x^2 + 1 \rangle, x + \langle x^2 + 1 \rangle, 2x + \langle x^2 + 1 \rangle, x + 1 + \langle x^2 + 1 \rangle, x + 2 + \langle x^2 + 1 \rangle, 2x + 1 + \langle x^2 + 1 \rangle, 2x + 2 + \langle x^2 + 1 \rangle \}

Definition. Let \( E \) be an extension field of \( F \) and let \( f(x) \in F[x] \). We say \( f(x) \) splits in \( E \) if \( f(x) \) can be factored as a product of linear factors in \( E[x] \). We call \( E \) a splitting field for \( f(x) \) over \( F \) if \( f(x) \) splits in \( E \) but in no proper subfield of \( E \).

Examples. (1) \( f(x) = x^2 + 1 \in \mathbb{Q}[x] = (x + i)(x - i) \) so \( f(x) \) splits in \( \mathbb{C} \). However \( \mathbb{Q}[i] = \{ a + bi | a, b \in \mathbb{Q} \} \) is the splitting field of \( f(x) \) over \( \mathbb{Q} \). \( f(x) = x^2 + 1 \in \mathbb{R}[x] \). \( \mathbb{R}[i] = \{ a + bi | a, b \in \mathbb{R} \} \) is the splitting field of \( f(x) \) over \( \mathbb{R} \).
(2) \( x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2}) \) split in \( \mathbb{R} \) but a splitting field for \( f(x) \) is \( \mathbb{Q}[\sqrt{2}] = \{ r + s\sqrt{2} | r, s \in \mathbb{Q} \} \).
(3) \( f(x) = x^4 - x^2 - 2 = (x^2 - 2)(x^2 + 1) \) over \( \mathbb{Q} \). Zeros in \( \mathbb{C} \) are \( \pm \sqrt{2}, \pm i \). A splitting field of \( f(x) \) over \( \mathbb{Q} \) \( : \mathbb{Q}(\sqrt{2},i) = \mathbb{Q}(\sqrt{2})(i) = \{ \alpha + \beta i | \alpha, \beta \in \mathbb{Q}(\sqrt{2}) \} = \{ (a + b\sqrt{2}) + (c + d\sqrt{2})i \} \).

Notation. Let \( F \) be a field and let \( a_1, a_2, ..., a_n \) be elements of some extension \( E \) of \( F \). User \( F(a_1, a_2, ..., a_n) \) to denote the smallest subfield of \( E \) that contains \( F \) and the set \( \{ a_1, a_2, ..., a_n \} \). Also, if \( f(x) \in F[x] \) and \( f(x) \) factors as \( f(x) = b(x - a_1)(x - a_2)...(x - a_n) \) over some extension \( E \) of \( F \). Then \( F(a_1, ..., a_n) \) is a splitting field over \( F \) in \( E \).

Theorem 12.4. Let \( F \) be a field and \( p(x) \in F[x] \) an irreducible polynomial if \( a \) is root of \( p(x) \) then \( F(a) \cong F[x]/\langle p(x) \rangle \).

(This theorem was not given in class but was given during the homework session.)

13. Algebraic Field Extensions (by Tim Ferdinands)

Theorem 13.1. Let \( F \) be a field and \( P(x) \in F[x] \) be an irreducible polynomial over \( F \). If \( a \) is a zero of \( p(x) \) in some extension \( E \) of \( F \), then \( F(a) \) is isomorphic to \( F[x]/\langle p(x) \rangle \).

Proof. Consider \( \phi : F[x] \to F(a) \) given by \( \phi(f(x)) = f(a) \). We claim that \( \ker \phi = \langle p(x) \rangle \).

Since \( p(a) = 0, \langle p(x) \rangle \subseteq \ker \phi \). And since \( p(x) \) is irreducible, \( \langle p(x) \rangle \) is maximal by a prior theorem. So if \( \langle p(x) \rangle \subseteq \ker \phi \subseteq F[x] \),

then \( \ker \phi \neq F[x] \) because \( f(x) = 1 \) is not a kernel element. Thus \( \langle p(x) \rangle = \ker \phi \).

When \( F \) is a field and \( p(x) \) is irreducible \( F[x]/\langle p(x) \rangle \) is a field. By the first isomorphism theorem \( F[x]/\langle p(x) \rangle \cong F(a) = \phi(F[x]) \).

Definition. Let \( E \) be an extension field of a field \( F \) and let \( a \in E \). We call \( a \) algebraic over \( F \) if \( a \) is the zero of a some nonzero polynomial in \( F[x] \).

If \( a \) is not algebraic over \( F \) it is called transcendental over \( F \). An extension \( E \) of \( F \) is called an algebraic extension of \( F \) if every element of \( E \) is algebraic over \( F \).

Example. \( \sqrt{2} \) is algebraic over \( \mathbb{Q} \). \( f(x) = x^2 - 2 \). \( \mathbb{Q}(\sqrt{2}) = \{ a + b\sqrt{2} : a, b \in \mathbb{Q} \} \) is an algebraic extension.

Definition. \( F[x] = \left\{ \frac{f(x)}{g(x)} | f(x), g(x) \in F[x] \right\} \) is the field of quotients of \( F[x] \).
Theorem 13.2. Let $E$ be an extension field of the field $F$ with $a \in E$. If $a$ is transcendental over $F$, then $F(a) \cong F[x]$.

If $a$ is algebraic over $F$ then

$$F(a) \cong F[x]/(p(x))$$

where $p(x)$ is a polynomial of minimum degree such that $p(a) = 0$. Moreover $p(x)$ is irreducible over $F$.

Proof. Consider

$$\phi : F[x] \rightarrow F(a)$$

by

$$\phi(f(x)) = f(a).$$

If $a$ is transcendental over $F$, then $\ker \phi = \{0\}$ and we have an isomorphism

$$\tilde{\phi} : F[x] \rightarrow f(a)$$

by

$$\tilde{\phi} : \frac{f(x)}{g(x)} = \frac{f(a)}{g(a)}.$$

Now if $a$ is algebraic over $F$, then $\ker \phi \neq 0$ because $f(a) = 0$ for some nonzero $f(x)$ and there is some polynomial $p(x)$ in $F[x]$ such that $\ker \phi = \langle p(x) \rangle$. $p(x)$ has minimal degree among elements of $\ker \phi$. By the first isomorphism theorem

$$F(a) \cong F[x]/(p(x)).$$

$\square$

Definition. Let $E$ be an extension field of $F$. We say that $E$ has degree $n$ over $F$ and write $[E : F] = n$ if $E$ has dimension $n$ as a vector space over $F$. If $[E : F]$ is finite, $E$ is called a finite extension of $F$.

Otherwise $E$ is an infinite extension.

Example. $\mathbb{C} = \{a + bi | a, b \in \mathbb{R}\}$ has basis $\{1, i\}$ as a vector space over $\mathbb{R}$. So $[\mathbb{C} : \mathbb{R}] = 2$.

On the other hand, $\mathbb{C}$ has infinite degree over $\mathbb{Q}$.

Example. $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$. $\{1, \sqrt{2}\}$ is a basis for $\mathbb{Q}(\sqrt{2})$. Thus $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

Theorem 13.3. If $E$ is a finite extension of $F_1$, then $E$ is an algebraic extension of $F$.

Proof. Suppose $[E : F] = n$ and $a \in E$. Then $\{1, a, \ldots, a^n\}$ is linearly dependent over $F$. Thus there are elements $c_0, c_1, \ldots, c_n \in F$ such that $c_0 + c_1 a + c_2 a^2 + \cdots + c_n a^n = 0$ with not all $c_i = 0$.

So $f(x) = c_0 + c_1 + \cdots + c_n x^n$ is a nonzero polynomial that has $a$ for a root. Thus $a$ is algebraic over $F$. $\square$

Theorem 13.4. Let $K$ be a finite extension field of $E$ and let $E$ be a finite extension field of $F$. Then $K$ is a finite extension field of $F$ and

$$[K : F] = [K : E][E : F].$$

Proof. Let $X = \{x_1, x_2, \ldots, x_n\}$ be a basis for $K$ over $E$. So $[K : E] = n$, and let $Y = \{y_1, y_2, \ldots, y_n\}$ be a basis for $E$ over $F$, so $[E : F] = m$.

We claim that

$$YX = \{y_j x_i | 1 \leq j \leq m, 1 \leq i \leq n\}$$

is a basis for $K$ over $F$.

Choose $a \in K$. Then there are elements $b_1, b_2, \ldots, b_n \in E$ such that

$$a = b_1 x_1 + b_2 x_2 + \cdots + b_n x_n.$$
For each \(i = 1, 2, \ldots, n\) there are \(c_{i_1}, c_{i_2}, \ldots, c_{i_m}\) such that
\[
b_i = c_{i_1}y_1 + c_{i_2}y_2 + \cdots + c_{i_m}y_m.
\]

\[
a = \sum_{i=1}^{n} b_i x_i = \sum_{i=1}^{n} \left( \sum_{j=1}^{m} c_{i_j} y_i \right) x_i = \sum_{i,j} c_{i_j} (y_j x_i)
\]

So \(XY\) spans \(K\) over \(F\) (elements can be written as elements in \(F\)).
But is it linearly independent?

\[
\sum_{i,j} c_{i_j} (y_j x_i) = \sum_i \left( \sum_{j} c_{i_j} y_j \right) x_i = 0
\]

Since \(X\) is a basis for \(K\) over \(E\) \(\sum_{i,j} c_{i_j} y_j = 0\). And since \(Y\) is a basis for \(E\) over \(F\), \(\sum_{i,j} c_{i_j} y_j = 0\), and \(c_{i_j} \in F\) means that \(c_{i_j} = 0\). Thus we have linear independence. Therefore \(y_j x_i\) form a basis for \(K\) over \(F\).

\[\square\]

14. CYCLOTOMIC POLYNOMIALS AND GROUP RINGS (BY JAYNA RESMAN)

Cyclotomic Polynomials.

- The complex zeros of \(x^n - 1\) are 1 and those of the form \(\omega = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right)\).
- \(Q\) forms a cyclic group of order \(n\). The generators are of the form \(\omega^k\) for \(1 \leq k \leq n\) and \(gcd(k, n) = 1\). These are called the \(n\)th roots of unity.
- \(\phi(n) = \#\) of integers, \(k\), less than or equal to \(n\) with \(gcd(n, k) = 1\)
- \(Q(\omega) = \) splitting field of \(x^n - 1\) called the \(n\)th cyclotomic extension of \(Q\).
- The irreducible factors of \(x^n - 1\) over \(Q\) are cyclotomic polynomials.

Definition. For any positive integer \(n\), let \(\omega_1, \ldots, \omega_{\phi(n)}\) be the primitive roots of unity. The \(n\)th cyclotomic polynomial over \(Q\) is the polynomial \(\phi_n(x) = (x - \omega_1)(x - \omega_2)\cdots(x - \omega_{\phi(n)})\) where \(\omega_1 = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right)\).

Examples.

- For \(n = 1\), \(\omega = \cos\left(\frac{2\pi}{1}\right) + i \sin\left(\frac{2\pi}{1}\right) = 1\). Therefore \(\phi_1(x) = (x - 1)\).
- For \(n = 2\), \(\omega = \cos\left(\frac{2\pi}{2}\right) + i \sin\left(\frac{2\pi}{2}\right) = -1\). Therefore \(\phi_2(x) = (x + 1)\).
- For \(n = 3\), \(\omega_1 = \cos\left(\frac{2\pi}{3}\right) + i \sin\left(\frac{2\pi}{3}\right) = \frac{-1}{2} + \frac{\sqrt{3}}{2} i\) and

\[
\omega_2 = \omega_1^2 = \left(-\frac{1}{2} + \frac{\sqrt{3}}{2} i\right) \left(-\frac{1}{2} + \frac{\sqrt{3}}{2} i\right) = -1 - \frac{\sqrt{3}}{2} i.
\]

Therefore, \(\phi_3(x) = \left(x - \left(-\frac{1}{2} + \frac{\sqrt{3}}{2} i\right)\right) \left(x - \left(-\frac{1}{2} - \frac{\sqrt{3}}{2} i\right)\right) = x^2 + x + 1\).

Theorem 14.1. For every \(n \in \mathbb{N}\), \(x^n - 1 = \prod_{d|n} \phi_d(x)\) where the product runs over all possible divisors, \(d\), of \(n\).

Example. \(x^3 - 1 = \phi_1(x)\phi_3(x) = (x - 1)(x^2 + x + 1)\).

Theorem 14.2. The cyclotomic polynomials \(\phi_n(x)\) are irreducible over \(\mathbb{Z}\).

Group Rings.

- Fix a commutative ring \(R\) with unity 1, and let \(G = \{g_1, g_2, \ldots, g_n\}\) be any finite group with multiplication. The group ring \(R[G]\) with coefficients in \(R\) is the set of formal sums: \(a_1 g_1 + a_2 g_2 + \cdots + a_n g_n\) with \(a_i \in R\).
- If \(g_1\) is the multiplicative identity in \(G\), then \(a_i g_1 = a_i\) and \(1 \cdot g_j = g_j\) for all \(g_j \in G\).
- Addition is component-wise.

\[
(a_1 g_1 + a_2 g_2 + \cdots + a_n g_n) + (b_1 g_1 + b_2 g_2 + \cdots + b_n g_n) = (a_1 + b_1) g_1 + (a_2 + b_2) g_2 + \cdots + (a_n + b_n) g_n
\]

- Multiplication

\[
(a_1 g_1 + a_2 g_2 + \cdots + a_n g_n)(b_1 g_1 + b_2 g_2 + \cdots + b_n g_n) = \sum a_i b_j g_k \text{ where } (g_k = g_i g_j).
\]
Example. Recall the Quaternion group $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$. Then $2i - 3j$ and $4 + 2k - j$ are both elements in $\mathbb{Z}[Q_8]$.

**Theorem 14.3.** If $R$ is a subring of $S$, then $R[G]$ is a subring of $S[G]$ for any group $G$.

**Proof.** First note that $R[G]$ is non-empty since $R$ is a ring (and thus contains an additive identity) and $G$ is a group (and thus contains its own identity). Let $\alpha, \beta \in R[G]$ and $\alpha = (a_1 g_1 + a_2 g_2 + \ldots + a_n g_n), \beta = (b_1 g_1 + b_2 g_2 + \ldots + b_n g_n)$ such that $a_i, b_i \in R$ and $a_i \in S$. Therefore, $(a_1 g_1 + a_2 g_2 + \ldots + a_n g_n) \in S[G]$, too.

$$\alpha - \beta = (a_1 - b_1) g_1 + (a_2 - b_2) + \ldots + (a_n - b_n) g_n$$

But, $(a_i - b_i) \in R$, thus $\alpha - \beta \in R[G]$.

$$\alpha \beta = \left(\sum a_i g_i \right) \left(\sum b_j g_j \right) = \sum a_i b_j g_k,$$

and $a_i, b_j \in R$, thus $\alpha \beta \in R[G]$. Thus, $R[G]$ is non-empty and closed under subtraction and multiplication, so $R[G]$ is a subring of $S[G]$. \qed

**Definition.** A ring $R$ with unity is called reversible if $ab = 0$ implies $ba = 0$ for all $a, b \in R$.

**Definition.** A ring $R$ with unity is called symmetric if $abc = acb$ for all $a, b, c \in R$.

**Appendix: Notes from David Jorgensen (by Becky Egg)**

**Two ways to study rings**

- inside:
  - Does the ring have
    - zero divisors?
    - idempotents?
  
  - What is the
    - radical of an ideal?
    - the Jacobson radical (the intersection of all maximal left ideals)?
    - the nilradical (the set of all nilpotent elements)?
    - ideals?

- outside:
  - modules
  - free modules
  - projective modules
  - injective modules
  - flat modules
  - extensions
  - functors
  - derived functors

**an analogy for modules:**

\[
\begin{align*}
\text{an analogy for modules:} & & \text{k a field} & & \text{R a ring} \\
& & \text{V a vector space} & & \text{M a module} \\
& & \text{linear transformations} & & \text{R-module homomorphisms}
\end{align*}
\]

**Example.** $\mathbb{R}^n = \{(a_1, a_2, \ldots, a_n) | a_i \in \mathbb{R}\}$ is a vector space over $\mathbb{R}$.

**Definition.** A left $R$-module $M$ is an abelian group under $+$ along with ring multiplication $r \cdot x$ such that the following axioms hold: For all $r, s \in R$ and all $x, y \in M$

1. $r \cdot x \in M$ (closure)
2. $r \cdot (x + y) = r \cdot x + r \cdot y \quad (r + s) \cdot x = r \cdot x + s \cdot x$ (distributive properties)
3. $r \cdot (s \cdot x) = (rs) \cdot x$ (associativity)
4. $1_R \cdot x = x$.

In addition, if $1_R \in R$, then
If (4) holds, then $M$ is called a unitary module over $R$.

**Example.**

1. $R$ is itself an $R$-module.
2. $I$ an ideal of $R$ is an $R$-module.
3. $R/I$ is an $R$-module.
4. $R^n = R \times R \times \cdots \times R = \{(a_1, \ldots, a_n) | a_i \in R\}$ is an $R$ module, where the operations are defined componentwise. In fact, $R^n$ is a free module.

**Definition.** A subset $\{x_\lambda\}_{\lambda \in \Lambda}$ of an $R$-module $M$ is a generating set for $M$ if

$$M = \{r_1 x_{\lambda_1} + r_2 x_{\lambda_2} + \cdots + r_n x_{\lambda_n} | r_i \in R\},$$

i.e., $M$ is the set of finite $R$-linear combinations of elements of $\{x_\lambda\}_{\lambda \in \Lambda}$.

If there exists a generating set $\{x_\lambda\}_{\lambda \in \Lambda}$ such that $|\Lambda| < \infty$, then $M$ is called a finitely generated module. [Note that in our analogy between modules and vector spaces, a generating set corresponds to a spanning set.]

**Definition.** The set $\{x_\lambda\}_{\lambda \in \Lambda}$ is linearly independent if for all $x_{\lambda_1}, \ldots, x_{\lambda_n},$

$$r_1 x_{\lambda_1} + \cdots + r_n x_{\lambda_n} = 0$$

implies $r_1 = \cdots = r_n = 0$.

**Definition.** An $R$-module $M$ is called free if it has a linearly independent generating set, called a basis.

**Example.** Consider the following $\mathbb{Z}$-modules:

1. For $n \in \mathbb{N}$, $\mathbb{Z}^n$ is a free module.
2. (2) is generated by 2. Note that $r \in \mathbb{Z}$ with $r2 = 0$ implies that $r = 0$, so $\{2\}$ is a basis, and hence (2) is a free module.
3. (2, 3) = $\mathbb{Z}$ is also a free module, with basis $\{1\}$.
4. $M = \mathbb{Z}/(2) = \{0 + (2), 1 + (2)\}$ is a $\mathbb{Z}$-module; its only generating set is $\{1 + (2)\}$. Note however that $2(1 + (2)) = 2 + (2) = (2) = 0_{\mathbb{Z}/(2)}$.

so $\mathbb{Z}/(2)$ is finitely generated, but not a free module.

**Example.** Let $k$ be a field, and consider the following $k[x, y]$-modules:

1. $M = (x)$ is a module with generating set $\{x\}$. Since $r(x, y)x = 0$ implies that $r(x, y) = 0$, $M$ is a free module.
2. $N = (x, y)$ is generated by $\{x, y\}$. Note however that $(-y)x + (x)y = 0$, so $N$ is not a free module.

If turns out that every $R$-module $M$ “looks like” (i.e., is isomorphic to) $F/S$, where $F$ is a free module, and $S$ is a submodule of $F$.

**Exercises:** Let $k$ be a field and $G = \langle g \rangle$ be a cyclic group of order 2. Let $R = k[G]$.

1. Let

$$M = \left\{ \begin{bmatrix} \alpha \\ \beta \end{bmatrix} | \alpha, \beta \in k \right\}.$$ 

Determine which of the following define $R$-modules; justify your answers.

(a)

$$ e \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha \\ 0 \end{bmatrix}, \quad g \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} 0 \\ \beta \end{bmatrix}$$

(b)

$$ e \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}, \quad g \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha + 1 \\ \beta + 1 \end{bmatrix}$$

(c)

$$ e \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}, \quad g \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha \\ 0 \end{bmatrix}$$
Now let
\[
M = \left\{ \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{bmatrix} \mid \alpha, \beta, \gamma, \delta \in k \right\},
\]
and determine which of the following define \( R \)-modules:

\[
\begin{align*}
(e) \quad e \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{bmatrix} &= \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{bmatrix}, \\
g \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{bmatrix} &= \begin{bmatrix} \beta \\ \alpha \\ \delta \\ \gamma \end{bmatrix}
\end{align*}
\]

\[
(f) \quad e \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{bmatrix} &= \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{bmatrix}, \\
g \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{bmatrix} &= \begin{bmatrix} \delta \\ \alpha \\ \beta \\ \gamma \end{bmatrix}
\]

(2) Of the modules given in (1), determine which are free modules.

(3) A representation of a group \( G \) is a group homomorphism \( \rho : G \to GL(V) \), where \( V \) is a finite dimensional vector space over a field \( k \) and \( GL(V) \) is the set of invertible linear transformations from \( V \) to \( V \). If \( \dim V = n \), then \( \rho \) is an \( n \)-dimensional representation.

Define a bijective correspondence between \( n \)-dimensional representations of \( G \) and \( n \)-dimensional \( k[G] \)-modules.

Let \( R \) be an associative ring with 1.

Recall the correspondence between a vector space over a field and a module of a ring. Free modules, i.e., those which have a basis, have the clearest correspondence to vector spaces over a field.

**Definition.** A subset \( S \) of an \( R \)-module \( M \) is called a submodule of \( M \) if it is an \( R \)-module whose ring multiplication is compatible with that of \( M \).

**Definition.** A function \( f : M \to N \) between \( R \)-modules \( M \) and \( N \) is called an \( R \)-module homomorphism if for all \( x, y \in M \) and all \( r \in R \)

\[
\begin{align*}
(1) \quad f(x + y) &= f(x) + f(y) \\
(2) \quad f(rx) &= rf(x).
\end{align*}
\]

**Exercises:**

(1) Let \( f : M \to N \) be an \( R \)-module homomorphism. Show that \( \ker f \) and \( \text{im}(f) \) are \( R \)-submodules of \( M \) and \( N \), respectively.

(2) If \( N \) is a submodule of the \( R \)-module \( M \), then \( M/N \) is also an \( R \)-module.

**Theorem 14.4.** Every \( R \)-module is the homomorphic image of a free module.

**Proof.** Let \( M \) be an \( R \)-module and \( \{x_\lambda\}_{\lambda \in \Lambda} \) be a generating set for \( M \). Let \( F \) be the free \( R \)-module on the basis \( \{e_\lambda\}_{\lambda \in \Lambda} \). Define

\[
f : F \to M \\
e_\lambda \mapsto x_\lambda,
\]
and extend by linearity (i.e., \( f(r_1 e_{\lambda_1} + \cdots + r_n e_{\lambda_n}) = r_1 x_{\lambda_1} + \cdots + r_n x_{\lambda_n} \)). By construction, \( f \) is a surjective homomorphism. \( \square \)
Using the first isomorphism theorem, we have the following:

**Corollary 14.5.** \( M \cong F/S, \) where \( S = \ker f, \) with \( f \) given above.

This result is the first step in the idea of a ‘free resolution’, the ultimate determination in the failure of a module to be free.

**Definition.** A sequence

\[
L \xrightarrow{f} M \xrightarrow{g} N
\]

of \( R \)-module homomorphisms is called **exact** if \( \ker g = \text{im} f \).

**Example.**

\[
0 \rightarrow S_1 \xrightarrow{\subseteq} F_0 \xrightarrow{f} M \rightarrow 0
\]

is a short exact sequence. Note that since the image of the injection from \( S_1 \) to \( F_0 \) is all of \( S_1 \), we have that \( \ker f = S_1 \).

We can repeat this process on \( S_1 \):

\[
0 \rightarrow S_2 \rightarrow F_1 \rightarrow S \rightarrow 0,
\]

and then splice or compose these two sequences to get

\[
F_1 \xrightarrow{d_1} F_0 \xrightarrow{\pi} M \rightarrow 0
\]

The above sequence is exact, and called a **free presentation** of \( M \). If \( F_1, F_0 \) are finitely generated free modules, then \( M \) is called **finitely presented**.

Suppose that \( M \) is finitely presented. Then \( F_1, F_0 \) are finitely generated free modules; let \( F_1 \) be of rank \( n \), and \( F_0 \) be of rank \( m \). Then we can represent the \( R \)-module homomorphism \( d_1 \) by an \( m \times n \) matrix, with entries in \( R \)

\[
d_1 = \begin{bmatrix}
r_{11} & r_{12} & \cdots & r_{1n} \\
r_{21} & r_{22} & \cdots & r_{2n} \\
\vdots & \vdots & \ddots & \vdots \\
r_{m1} & r_{m2} & \cdots & r_{mn}
\end{bmatrix},
\]

where this matrix is given with respect to the bases \( \{e_1, \ldots, e_n\} \) of \( F_1 \) and \( \{e'_1, \ldots, e'_m\} \) of \( F_0 \). Then we have

\[
\pi(d_1(e_1)) = \pi(r_{11}e'_1 + r_{21}e'_2 + \cdots + r_{m1}e'_m)
= r_{11}x_1 + r_{21}x_2 + \cdots + r_{m1}x_m
= 0.
\]

This non-trivial 0-linear combination shows that \( x_1, \ldots, x_m \) are not linearly independent, i.e., \( M \) is not a free module.

In fact, the column space of \( d_1 \) generates all the nontrivial linear relations of the generators of \( M \). “All” the information about \( M \) is contained in the presentation matrix \( d_1 \).

We can continue this process:

\[
0 \rightarrow S_2 \rightarrow F_1 \xrightarrow{d_1} F_0 \rightarrow M \rightarrow 0,
\]

which we compose to get

\[
F_2 \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \rightarrow M \rightarrow 0.
\]

What we’ve just constructed is called a **free resolution**.
Definition. A free resolution of an R-module M is an exact sequence
\[ \cdots \xrightarrow{d_n} F_n \xrightarrow{d_{n-1}} \cdots \xrightarrow{d_2} F_2 \xrightarrow{d_1} F_1 \xrightarrow{d_0} F_0 \xrightarrow{d_{-1}} F_{-1} \xrightarrow{d_{-2}} \cdots \to M \to 0, \]
where each \( F_i \) above is a free R-module.

Example. (1) \( R = f[x,y], M = (x,y) \). We have
\[ S_1 \xrightarrow{d_2} R^2 \xrightarrow{d_1} M \xrightarrow{d_0} 0, \]
where the map from \( R^2 \) to \( M \) is given by
\[ e_1 \mapsto x \]
\[ e_2 \mapsto y, \]
and \( e_1, e_2 \) are the standard basis vectors for \( R^2 \). A vector \( \begin{pmatrix} a \\ b \end{pmatrix} \) maps to \( ax + by \), so for \( \begin{pmatrix} a \\ b \end{pmatrix} \) in the kernel of this map, we have \( a = -a' y, b = -a' x \), i.e.,
\[ \begin{pmatrix} a \\ b \end{pmatrix} = a' \begin{pmatrix} -y \\ x \end{pmatrix}. \]
Thus \( \begin{pmatrix} -y \\ x \end{pmatrix} \) generates the kernel of this map. Thus \( S_1 = \begin{pmatrix} -y \\ x \end{pmatrix} \). Since this is a one-dimensional module, we have
\[ R \xrightarrow{d_2} S_1 \xrightarrow{d_1} 0, \]
given by \( e_1 \mapsto \begin{pmatrix} -y \\ x \end{pmatrix} \). Composing these sequences gives
\[ R \xrightarrow{d_2} R^2 \xrightarrow{d_1} M \xrightarrow{d_0} 0. \]
Note that if \( a \in \ker d_2 \), then
\[ a \begin{pmatrix} -y \\ x \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \]
implies that \( a = 0 \). So \( \ker d_2 = \{0\} \), and hence
\[ 0 \xrightarrow{d_0} R \xrightarrow{d_2} R^2 \xrightarrow{d_1} M \xrightarrow{d_0} 0 \]
is a free resolution of \( M \).

(2) \( R = k[x,y], M = R/(x,y) \), which is generated by \( 1 + (x,y) \). We have
\[ (x,y) \xrightarrow{e_1} R \xrightarrow{d_1} M \xrightarrow{d_0} 0, \]
where the map from \( R \) to \( M \) is given by \( e_1 \mapsto T \). Since we previously found the free resolution of \((x,y)\), we have
\[ 0 \xrightarrow{d_0} R \xrightarrow{d_2} R^2 \xrightarrow{d_1} M \xrightarrow{d_0} 0. \]

(3) Resolutions need not be finite: \( R = k[X,Y]/(X,Y), M = (x) \) and \( x = X + (XY) \). We have
\[ 0 \xrightarrow{d_0} (y) \xrightarrow{d_1} R \xrightarrow{d_0} M \xrightarrow{d_1} 0, \]
where the map from \( R \) to \( M \) is given by \( e_1 \mapsto x \). This resolution is infinite:
\[ \cdots \xrightarrow{d_2} R \xrightarrow{d_1} \cdots \xrightarrow{d_0} R \xrightarrow{d_{-1}} M \xrightarrow{d_{-2}} 0. \]
The modules \( S_i \) given in a free resolution are called syzygy modules of \( M \).

Definition. A complete resolution of an \( R \)-module \( M \) is an exact sequence
\[ F : \cdots \xrightarrow{d_2} F_2 \xrightarrow{d_1} F_1 \xrightarrow{d_0} F_0 \xrightarrow{d_{-1}} F_{-1} \xrightarrow{d_{-2}} \cdots, \]
where the \( F_i \)'s are finitely generated, \( M = \text{im}(d_0) \), and \( \text{hom}_R(F,R) \) is exact.
Example. The previous example

\[ \cdots \longrightarrow R \xrightarrow{[y]} R \xrightarrow{[x]} R \xrightarrow{[y]} R \longrightarrow M \longrightarrow 0. \]

is a complete resolution.

Exercises:

1. Compute the free resolutions of all the modules from yesterday’s problem 1.
2. Let \( k \) be a field.
   (a) Let \( R = k[G] \) where \( G = \langle g \rangle \) is a cyclic group of order 2. Let \( M = \langle e - g \rangle \). Find the complete resolution of this ideal.
   (b) Let \( R = k[G] \), where \( G = \langle g_1 \rangle \times \langle g_2 \rangle \) and \( g_1, g_2 \) are of order 2. Compute the free resolution of \( M = \langle e_1 - g_1, e_2 - g_2 \rangle \). Hint: consider example 2.
3. Two resolutions \( \rho_1 : G \to GL(V) \) and \( \rho_2 : G \to GL(W) \) are called equivalent if there exists and isomorphism \( \alpha : V \to W \) such that for all \( g \in G \),
   \[ \alpha \circ \rho_1(g) \circ \alpha^{-1} = \rho_2(g). \]

Show that the equivalence classes of \( n \)-dimensional representations are in bijective correspondence to the isomorphism classes of \( n \)-dimensional \( k[G] \)-modules.