MA 450: Honors Abstract Algebra Notes

Lecturer: Linquan Ma
Transcribed by Josh Park

Fall 2024

Contents

Lecture 24 (10/21)

10 Group Homomorphisms

Definition 1 (homomorphism)
A *homomorphism* $\phi : G \to \bar{G}$ between two groups is a mapping that preserves the group operation:

$$\phi(ab) = \phi(a)\phi(b) \quad \forall a, b \in G.$$

Definition 2 (kernel)
The *kernel* of a homomorphism $\phi : G \to \bar{G}$ is the set

$$\ker(\phi) = \{x \in G \mid \phi(x) = \bar{e}\}.$$

Example 1
Any isomorphism is a homomorphism with $\ker \phi = \{e\}$.

Examples

- $\phi : \mathrm{GL}(2, \mathbb{R}) \to (\mathbb{R}^*, \cdot)$ where $A \mapsto \det(A)$.

  Then $\phi(AB) = \det(AB) = \det(A)\det(B) = \phi(A)\phi(B)$ and $\ker \phi = \mathrm{SL}(2, \mathbb{R})$.
- $\phi : \mathbb{Z} \to \mathbb{Z}_n$ where $x \mapsto x \bmod n$.

  Then $\ker \phi = \langle n \rangle = n\mathbb{Z}$
- $\phi : (\mathbb{R}^*, \cdot) \to (\mathbb{R}^*, \cdot)$ where $x \mapsto x^2$.

  Then $\phi(xy) = (xy)^2 = x^2y^2 = \phi(x)\phi(y)$ and $\ker \phi = \{-1, 1\}$

Non-Examples

- $\phi : (\mathbb{R}, +) \to (\mathbb{R}, +)$ where $x \mapsto x^2$. Notice that

$$\begin{aligned} \phi(x + y) &= (x + y)^2 \\ &\neq \phi(x) + \phi(y) = x^2 + y^2 \end{aligned}$$

  so ϕ is <u>not</u> a homomorphism.
- $\phi : \mathbb{Z}_3 \to \mathbb{Z}_6$ where $x \mapsto 3x \bmod 6$

$$\begin{aligned} \phi(x + y) &= [3(x + y \bmod 3)] \bmod 6 \\ \phi(x) + \phi(y) &= [(3x \bmod 6) + (3y \bmod 6)] \bmod 6 \end{aligned}$$

  Now let $x = 1$ and $y = 2$. Then $\phi(1 + 2) = 0$ but $\phi(x) + \phi(y) = (3 + 0) \bmod 6 = 3$. Thus ϕ is <u>not</u> a homomorphism

Theorem 10.1 (Properties of elements under homomorphism)
Let $\phi : G \to \bar{G}$ be a homomorphism. Then

1. $\phi(e) = \bar{e}$
2. $\phi(g^n) = \phi(g)^n \quad \forall g \in G$
3. $|g|$ finite $\implies |\phi(g)| \mid |g|$
4. $\ker \phi \leq G$
5. $\phi(a) = \phi(b) \iff a \cdot \ker \phi = b \cdot \ker \phi$
6. $\phi(g) = g' \implies \phi^{-1}(g') = \{x \in G \mid \phi(x) = g'\} = g \cdot \ker \phi$

Example 2
Any homomorphism $\phi_i : \mathbb{Z}_3 \to \mathbb{Z}_6$ is determined by $\phi(1)$.

Note that $|\phi(1)| \bigm| |1| = 3 \implies |\phi(1)| = 1$ or $|\phi(1)| = 3$

$$\begin{aligned}
|\phi(1)| = 1 &\implies \phi(1) = 0 \implies \phi(x) = 0\ \forall x \quad \text{(i.e. } \phi \text{ is the trivial homomorphism)}\\
|\phi(1)| = 3 &\implies \phi(1) = 2 \text{ or } \phi(1) = 4\\
\phi(1) = 2 &\implies \phi(x) = 2x \bmod 6\\
\phi(1) = 4 &\implies \phi(x) = 4x \bmod 6
\end{aligned}$$

Example 3
Any homomorphism $\phi_i : \mathbb{Z}_m \to \mathbb{Z}_n$ is determined by $\phi(1)$.

$$\left.\begin{array}{l} |\phi(1)| \bigm| m \\ |\phi(1)| \bigm| n \end{array}\right\} \implies |\phi(1)| \bigm| \gcd(m,n)$$

Exercise
For all $g \in \mathbb{Z}_n$ with $|y| \bigm| \gcd(m,n)$, $\exists$hom. $\phi : \mathbb{Z}_m \to \mathbb{Z}_n$ sending 1 to y (so, $\phi(x) = xy \bmod n$).

Theorem 10.2 (Properties of sgps under homomorphisms)
Let $\phi : G \to \bar{G}$ be a homomorphism and $H \leq G$. Then

1. $\phi(H) = \{\phi(h) \mid h \in H\}$ is a sgp of $\bar{G}$
2. H cyclic $\implies \phi(H)$ cyclic
3. H abelian $\implies \phi(H)$ abelian
4. H normal $\implies \phi(H) \lhd \phi(G)$
5. $|\ker \phi| = n \implies \phi$ is an n-to-1 mapping from G onto $\phi(G)$
6. $|H| = n \implies |\phi(H)| \bigm| n$
7. $\overline{K} \leq \overline{G} \implies \phi^{-1}(\overline{K}) = \{k \in G \mid \phi(k) \in \overline{K}\} \leq G$
8. $\overline{K} \lhd \overline{G} \implies \phi^{-1}(\overline{K}) \lhd G$
   ($\implies$ **Cor:** $\ker \phi = \phi^{-1}(\bar{e}) \lhd G$)
9. ϕ is injective $\iff \ker \phi = \{e\}$
   ϕ is an isomorphism $\iff \phi$ is onto and $\ker \phi = \{e\}$

Examples
- $\phi : \mathbb{Z}_3 \to \mathbb{Z}_6$, $\quad \phi(1) = 4 \implies \phi(2) = 2,\ \phi(0) = 0$
  $\implies \ker \phi = \{0\}$. ϕ is 1-1 but not onto.
- $\phi : \mathbb{Z}_{12} \to \mathbb{Z}_{12}$, $\quad \phi(1) = 3 \implies \phi(x) = 3x \bmod 12$
  $\implies \ker \phi = \{0, 4, 8\} \implies \phi$ is 3-to-1 mapping e.g.

$$\begin{aligned}
\phi(2) = 6 \implies \phi^{-1}(6) &= 2 + \{0, 4, 8\}\\
&= \{2, 6, 10\}\\
\phi^{-1}(\langle 6 \rangle) = \phi^{-1}(\{0, 6\}) &= \{0, 2, 4, 6, 8, 10\}\\
&= \langle 2 \rangle \leq \mathbb{Z}_{12}
\end{aligned}$$

Theorem 10.3 (First Isomorphism Theorem)
Let $\phi : G \to \overline{G}$ be a group homomorphism. Then, the mapping $G/\ker\phi \mapsto \phi(G)$ where $g \cdot \ker \phi \mapsto \phi(g)$ is an isomorphism. That is, $G/\ker\phi \cong \phi(G)$.

Lecture 25 (10/23)

Example 4 (N/C Theorem)
Let $H \leq G$. Recall the *normalizer of H in G* and the *centralizer of H in G*,

$$\begin{aligned} N(H) &= \{x \in G \mid xHx^{-1} = H\} \\ C(H) &= \{x \in G \mid xhx^{-1} \in H, \ \forall h \in H\} \end{aligned}$$

(Note: $H \lhd G \implies N(H) = G \implies H \lhd N(H)$).

Consider the map $\phi : N(H) \to \mathrm{Aut}(H)$ given by $g \mapsto \phi_g$, where ϕ_g is the inner automorphism of H induced by g. That is, $\phi_g(h) = ghg^{-1}$ for all $h \in H$.

Exercise
Check ϕ_g is an automorphism of H and check ϕ is a homomorphism (i.e. $\phi_{g_1 g_2} = \phi_{g_1} \circ \phi_{g_2}$).

Then, $\ker \phi = \{g \in N(H) \mid \phi_g = id_H\} = \{g \in N(H) \mid ghg^{-1} = h, \ \forall h \in H\} = C(H)$. Note that elements of $C(H)$ commute with all elements of H. Thus by Thm 10.3, $N(H)/C(H)$ is isomorphic to a sgp of $\mathrm{Aut}(G)$.

Theorem 10.4
Every normal sgp of a group G is the kernel of a homomorphism of G. That is,

$$N \lhd G \implies N = \ker(\phi : G \to G/N)$$

Example 5
Let $G = D_4$. Recall that $Z(D_4) = \{R_0, R_{180}\} \lhd D_4$. Define

$$\begin{aligned} \phi : D_4 &\to D_4/Z(D_4) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \\ \{R_0, R_{180}\} &\mapsto (0,0) \\ \{R_{90}, R_{270}\} &\mapsto (1,0) \\ \{F_0, F_{90}\} &\mapsto (0,1) \\ \{F_{45}, F_{135}\} &\mapsto (1,1) \end{aligned}$$

Thus $\ker \phi = Z(D_4)$.

11 Fundamental Theorem of Finite Abelian Groups

Theorem 11.1 (Fundamental Theorem of Finite Abelian Groups)
Every finite abelian group is isomorphic to a direct product of cyclic groups of prime-power order. Moreover, the number of terms in the product and the order of the cyclic groups are uniquely determined by the group. That is, for some group $G \cong \mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_{p_2^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{n_k}}$ where the p_i's are (not necessarily distinct) primes, the prime powers $p_1^{n_1}, p_2^{n_2}, \ldots, p_k^{n_k}$ are uniquely determined by G.

Theorem 11.2 (Abelian groups of order p^k)
There is one abelian group of order p^k for each set of positive integers whose sum is k (called a partition of k)

Example 6

Let $k = 2$. The abelian groups of order p^2 are $\mathbb{Z}_{p^2}$ (2=2) and $\mathbb{Z}_p \oplus \mathbb{Z}_p$ (2 = 1+1)

Example 7

order of G	partitions of k	possible direct products for G
p	1	$\mathbb{Z}_p$
p^2	2	$\mathbb{Z}_{p^2}$
	$1+1$	$\mathbb{Z}_p \oplus \mathbb{Z}_p$
p^3	3	$\mathbb{Z}_{p^3}$
	$2+1$	$\mathbb{Z}_{p^2} \oplus \mathbb{Z}_p$
	$1+1+1$	$\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$
p^3	4	$\mathbb{Z}_{p^4}$
	$3+1$	$\mathbb{Z}_{p^3} \oplus \mathbb{Z}_p$
	$2+2$	$\mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2}$
	$2+1+1$	$\mathbb{Z}_{p^2} \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$
	$1+1+1+1$	$\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$

Example 8

How many abelian groups are there of order $1176 = 7^2 \cdot 3 \cdot 2^3$?

$$\begin{array}{rlllll} 7^2: & \mathbb{Z}_{49} & \text{or} & \mathbb{Z}_7 \oplus \mathbb{Z}_7 & & \\ 3: & \mathbb{Z}_3 & & & & \\ 2^3: & \mathbb{Z}_8 & \text{or} & \mathbb{Z}_4 \oplus \mathbb{Z}_2 & \text{or} & \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \end{array}$$

Thus groups of order 1176 are

$$\begin{array}{l} \mathbb{Z}_{49} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_8 \\ \mathbb{Z}_{49} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2 \\ \mathbb{Z}_{49} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \\ \mathbb{Z}_7 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_8 \\ \mathbb{Z}_7 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2 \\ \mathbb{Z}_7 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \end{array}$$

so there are 6 possible abelian groups of order 1176.

Thus $\mathbb{Z}_{1176} \cong \mathbb{Z}_{49} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_8$

Lecture 26 (10/25)

If $|G| = 8$, how do we know whether it is $\mathbb{Z}_8$ or $\mathbb{Z}_4 \oplus \mathbb{Z}_2$ or $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$?

We can use the algorithm for determining an abelian group of order p^n.

Step 1. Compute the orders of all elements of G

Step 2. Select an element a_1 of maximum order. Define $G_1 = \langle a_1 \rangle$ and set $i = 1$.

Step 3. If $|G| = |G_i|$, we can stop. Otherwise, increment i.

Step 4. Select an element a_i of maximum order p^k, such that $p^k \leq \frac{|G|}{|G_{i-1}|}$ and none of $a_i, a_i^p, a_i^{p^2}, \dots, a_i^{p^k-1}$ are in G_{i-1} (This guarantees a_iG_{i-1} has order p^k in G/G_{i-1}). Define $G_i = G_{i-1} \times \langle a_i \rangle$

Step 5. Return to step 3.

Eventually,

$$G = \underbrace{\langle a_1 \rangle \times \langle a_2 \rangle \times \cdots \times \langle a_{i-1} \rangle \times \langle a_i \rangle}_{G_i} \times \cdots \times \langle a_s \rangle$$

Note 1
Observe that $|a_1| \geq |a_2| \geq \cdots \geq |a_s|$

Example 9
Consider the group $U(30) = \{1, 7, 11, 13, 17, 19, 23, 29\}$.

Since $|U(30)| = 8 = 2^3$, possibilities are $\mathbb{Z}_8$, $\mathbb{Z}_4 \oplus \mathbb{Z}_2$, and $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Step 1. $\langle 7 \rangle = \{1, 7, 19, 13\} \implies |7| = |13| = 4, \quad |19| = 2$
$\langle 23 \rangle = \{1, 23, 19, 17\} \implies |23| = |17| = 4, \quad |11| = 2, \quad |29| = 2$

Step 2. $a_1 = 7, \quad G_1 = \langle a_1 \rangle = \langle 7 \rangle$

Step 3. $|G_1| = 4 < 8, \quad i = 1 \rightsquigarrow i = 2$

★ Step 4. Pick some a_2 such that $|a_2| \leq \frac{|U(30)|}{|G_1|} = 2$ and a_2 is not contained in $G_1 = \langle 7 \rangle$

Set $a_2 = 11$ and define $G_2 = g_1 \times \langle a_2 \rangle = \langle 7 \rangle \times \langle 11 \rangle$

Step 5. $|G_2| = 4 \cdot 2 = 8 = |U(30)|$

$\implies U(30) = \langle 7 \rangle \times \langle 11 \rangle \cong \mathbb{Z}_4 \oplus \mathbb{Z}_2 \quad \square$

We can use concrete examples to simplify the identification process

Example 10
$|U(30)| = 8$

We know it has (4 elements of order 4), (3 elements of order 2), and (1 element of order 1).

Our options are $\mathbb{Z}_8, \quad \mathbb{Z}_4 \oplus \mathbb{Z}_2, \quad \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

We can rule out $\mathbb{Z}_8$ as we do not have an element of order 8.

We can rule out $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ as all elements here have order 2 (excl. e).

Thus the structure must be $\mathbb{Z}_4 \oplus \mathbb{Z}_2$.

Example 11
If an abelian group G has order $16 = 2^4$

Suppose G has (12 elements of order 4), (3 elements of order 2), (1 elements of order 41)

Our options are $\mathbb{Z}_{16}, \quad \mathbb{Z}_8 \oplus \mathbb{Z}_2, \quad \mathbb{Z}_4 \oplus \mathbb{Z}_4, \quad \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2, \quad \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

We don't have any elements of order 16 or 8, so can easily eliminate $\mathbb{Z}_{16}$ and $\mathbb{Z}_8 \oplus \mathbb{Z}_2$

Not $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, as it has too many elements of order 2.

Not $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, as it has 8 elements of order 4 (and 7 elements of order 2).

Thus $G \cong \mathbb{Z}_4 \oplus \mathbb{Z}_4$

Corollary 11.1
Let G be a finite <u>abelian</u> group. If $m \,\big|\, |G|$, then G has a subgroup of order m.

So, the converse of Lagrange's Theorem holds for finite abelian groups.

Remark 1
This cor. does not hold if G is not abelian (e.g. A_4 does not have any subgroups of order 6).

Proof of Corollary. By FTFAG,

$$G \cong \mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_{p_2^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{n_k}} \implies |G| = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$$

Now,

$$m \,\big|\, |G| \implies m = p_{i_1}^{n_{i_1}} p_{i_2}^{n_{i_2}} \cdots p_{i_k}^{n_{i_k}} \qquad \text{where} \qquad p_{i_1}^{r_{i_1}} \,\big|\, p_{i_1}^{n_{i_1}} \quad (\text{i.e. } r_{i_j} \leq n_{i_j})$$

$\implies$ by FTCG, $\exists$ subgroup $\mathbb{Z}_{p_{i_j}^{n_{i_j}}}$ with order $p_{i_j}^{r_{i_j}}$

$\implies$ Take their direct product. This yields a subgroup of G of order m. $\square$

Example 12
Let $|G| = 72 = 3^2 \cdot 2^3$. Find a subgroup of order $12 = 3^1 \cdot 2^2$.

The possibilities are

$$\begin{array}{lll} \mathbb{Z}_8 \oplus \mathbb{Z}_9 & \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 & \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \\ \mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 & \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 & \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \end{array}$$

In $\mathbb{Z}_9 \oplus \mathbb{Z}_8$, a subgroup of order 12 would be the direct product of two subgroups of orders 3 and 4. Thus one subgroup of order 12 is: $\langle 3 \rangle \oplus \langle 2 \rangle$.

In $\mathbb{Z}_9 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2$,

$$\begin{array}{cccccccc} \mathbb{Z}_9 & \oplus & \mathbb{Z}_4 & \oplus & \mathbb{Z}_2 & & & \\ 3^2 & \cdot & 2^2 & \cdot & 2 & = 72 & & \\ 3 & \cdot & 2^2 & \cdot & 1 & = 12 & \implies & \langle 3 \rangle \oplus \langle 1 \rangle \oplus \langle 0 \rangle \\ 3 & \cdot & 2 & \cdot & 2 & = 12 & \implies & \langle 3 \rangle \oplus \langle 2 \rangle \oplus \langle 1 \rangle \end{array}$$

Similarly for $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$,

$$\begin{array}{cccccccccccc} \mathbb{Z}_3 & \oplus & \mathbb{Z}_3 & \oplus & \mathbb{Z}_2 & \oplus & \mathbb{Z}_2 & \oplus & \mathbb{Z}_2 & & & \\ 3 & \cdot & 3 & \cdot & 2 & \cdot & 2 & \cdot & 2 & = 72 & & \\ 3 & \cdot & 1 & \cdot & 2 & \cdot & 2 & \cdot & 1 & = 12 & \implies & \langle 1 \rangle \oplus \langle 0 \rangle \oplus \langle 1 \rangle \oplus \langle 1 \rangle \oplus \langle 0 \rangle \end{array}$$

Lecture 27 (10/28)

Recall the Fundamental Theorem of Finite Abelian Groups:

Theorem 11.3
Let G be a finite abelian group. Then,

$$G \cong \mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_{p_2^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{n_k}}$$

where the p_i's are (not necessarily distinct) primes.

Lemma 11.1
Let G be a finite abelian group of order $p^n m$ where $\gcd(p, m) = 1$. Then $G = H \times K$ where

$$H = \{x \in G \mid x^{p^n} = e\} \qquad\qquad K = \{x \in G \mid x^m = e\}$$

Moreover, $|H| = p^n$ and $|K| = m$.

Proof of Lemma 1. $H \lhd G$ and $K \lhd G$ (e.g. $x^{p^n} = e = y^{p^n} \implies (xy)^{p^n} = x^{p^n} y^{p^n} = e$).

To show $G = H \times K$, ETS

- $H \cap K = \{e\}$

- $G = HK$

If $x \in H \cap K$ then $x^{p^n} = e,\ x^m = e$.

Since $\gcd(p^n, m) = 1$, $\exists a, b \in \mathbb{Z}$ such that $ap^n + bm = 1$.

$$x = x^{ap^n + bm} = x^{ap^n} \cdot x^{bm} = e.$$

For any $y \in G$ we can write $y = y^{ap^n+bm} = y^{ap^n} \cdot y^{bm}$.

Then $y^{ap^n} \in K$ because $(y^a)^{p^n m} = e$ because $|G| = p^n m$ and similarly, $y^{bm} \in H$.

Thus we have shown $G = H \times K$.

Finally, $p^n m = |G| = |H| \cdot |K|$ but $p \nmid |K|$ (if $p \,\big|\, |K| \xRightarrow{\text{Cauchy}} \exists$ an element of K of order p)

Similarly, we have $m \nmid |H| \implies |H| = p^n$ and $|K| = m$ □

Lemma 11.2
Let G be an abelian group such that $|G| = p^n$ and $a \in G$ be an element of maximal order. Then $G = \langle a \rangle \times K$ for some group K.

Proof of Lemma 2. We can show this by induction. If $n = 1$, then $|G| = p$, then $G = \langle a \rangle = \langle a \rangle \times \langle e \rangle$.

Assume we have proved the lemma for all p^k such that $k < n$.

Choose $a \in G$ which has maximal order, say p^m for some $m \le n$. Then $x^{p^m} = e$ for all $x \in G$.

If $m = n$ then $G = \langle a \rangle = \langle a \rangle \times \langle e \rangle$ and we are done. So assume $m \neq n$.

Pick b of smallest order such that $b \notin \langle a \rangle$.

Claim 1. $\langle a \rangle \cap \langle b \rangle = \{e\}$
Proof of claim. $|b^p| < |b|$ so by our choice $b^p \in \langle a \rangle$ say $b^p = a^i$.

Then $e = b^{p^m} = (b^p)^{p^{m-1}} = (a^i)^{p^{m-1}}$ so $\left|a^i\right| \le p^{m-1} \implies a_i$ is not a generator for $\langle a \rangle$.

$\implies \gcd(p^m, i) \neq 1 \implies p \,\big|\, i$ and we can write $i = pj$ for some j.

Then $b^p = a^i = a^{pj}$, set $c = a^{-j} b$.

Then $c \notin \langle a \rangle$ (*because if* $c \in \langle a \rangle$, *then* $b \in \langle a \rangle$ *since* $b = a^j c$) and $c^p = a^{-jp} b^p = e$.

Thus we have found an element c of order p such that $c \notin \langle a \rangle$.

Since b has the smallest order such that $b \notin \langle a \rangle \implies |b| \le p$, but then $|b| = p$.

Then $\langle a \rangle \cap \langle b \rangle = \{e\}$ since otherwise elements in this intersection would generate $\langle b \rangle$ so $b \in \langle a \rangle$ ($\Rightarrow\Leftarrow$) ■

Next, consider the group $\overline{G} = G/\langle b \rangle$ and use $\bar{x}$ to denote $x\langle b \rangle \in \overline{G}$.

If $|\bar{a}| < |a| = p^m$ then $\bar{a}^{p^{m-1}} = \bar{e} \implies (a\langle b \rangle)^{p^{m-1}} = a^{p^{m-1}} \langle b \rangle = \langle b \rangle$ so $a^{p^{m-1}} \in \langle a \rangle \cap \langle b \rangle = \{e\}$ ($\Rightarrow\Leftarrow$)

Thus $|\bar{a}| = p^m \implies \bar{a}$ is an element with maximal order in $\overline{G}$.

By induction, $\overline{G} = \langle \bar{a} \rangle \times \overline{K}$ for some $\overline{K} \lhd \overline{G}$.

Let K be the pre-image of $\overline{K}$ under $\begin{matrix} G \to \overline{G} \\ K \to \overline{K} \end{matrix}$ (i.e. $K = \{x \in G \mid \bar{x} \in \overline{K}\}$)

Claim 2. $\langle a \rangle \cap K = \{e\}$
Proof. If $x \in \langle a \rangle \cap K$ then $\bar{x} \in \langle \bar{a} \rangle \cap \overline{K} = \{\bar{e}\} \implies x \in \langle b \rangle \implies x \in \langle a \rangle \cap \langle b \rangle = \{e\}$ by previous claim. ■

It remains to show that $\langle a \rangle K = G$.

$$|\langle a \rangle K| = |\langle a \rangle|\, |K| = |\langle \bar{a} \rangle|\, \left|\overline{K}\right| \cdot p = \left|\overline{G}\right| \cdot p = |G|$$

Note that $G \to \overline{G}$ is p-to-1 since $|\ker| = p$. Thus, $\langle a \rangle K = G$. Therefore $G = \langle a \rangle \times K$ □

Lecture 28 (10/30)

To recap last lecture, the **Fundamental Theorem of Finite Abelian Groups** states:

G finite abelian group $\implies |G| = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$

By **Lemma 1**, $G = G(p_1) \times G(p_2) \times \cdots \times G(p_k)$ where each $G(p_i)$ has order $p_i^{n_i}$.

By **Lemma 2**, each $G(p_i)$ = internal direct product of cyclic groups, each has order of some power of p_i

24 Sylow's Theorem

Definition 3 (Conjugate class of a)
$a, b \in G$ are called conjugate in G if $b = xax^{-1}$ for some $x \in G$.

The conjugate class of a is the set $\mathrm{cl}(a) = \{xax^{-1} \mid x \in G\}$.

Remark 2
Conjugacy is an equivalence relation on G.

Example 13
$D_4 = \{R_0,\ R_{90},\ R_{180},\ R_{270},\ F_0,\ F_{45},\ F_{90},\ F_{135}\}$

$$\mathrm{cl}(R_0) = \{R_0\} \qquad \mathrm{cl}(R_{90}) = \{R_{90}, R_{270}\} = \mathrm{cl}(R_{270}) \qquad \mathrm{cl}(R_{180}) = \{R_{180}\}$$
$$\mathrm{cl}(F_0) = \{F_0, F_{90}\} = \mathrm{cl}(R_{90}) \qquad \mathrm{cl}(F_{45}) = \{F_{45}, F_{135}\}$$

Theorem 24.1 (24.1)
Let G be a finite group and $a \in G$. Then, $|\mathrm{cl}(a)| = [G : C(a)]$.

Proof of Theorem 24.1. Recall $C(a) = \{h \in G \mid ha = ah\}$ is the centralizer of a in G and $C(a) \leq G$.

Consider $\begin{array}{c} G \to \mathrm{cl}(a) \\ x \mapsto xax^{-1} \end{array}$ induces a map $T : \begin{array}{r} \{\text{left cosets of } C(a)\} \to \mathrm{cl}(a) \\ xC(a) \mapsto xax^{-1} \end{array}$.

- T is well-defined if

$$\begin{aligned} xC(a) = yC(a) &\iff x = yh \text{ for some } h \in Ca \\ &\implies xax^{-1} = yhah^{-1}y^{-1} = yay^{-1} \end{aligned}$$

- T is onto (obvious)
- T is 1-1:

$$\begin{aligned} xax^{-1} = yay^{-1} &\implies (y^{-1}x)a = a(y^{-1}x) \\ &\implies y^{-1}x \in C(a) \\ &\implies xC(a) = yC(a) \end{aligned}$$

Since T is a 1-1 correspondence, we know that

$$|\mathrm{cl}(a)| = \#\text{ of left cosets of C(a)} = [G : C(a)] = \frac{|G|}{|C(a)|}$$

□

Corollary 24.1
$|\mathrm{cl}(a)| \mid |G|$ for any $a \in G$

Proof of Corollary. $|\mathrm{cl}(a)| = \frac{|G|}{|C(a)|} \Big| \, |G|$ □

Corollary 24.2
For any finite group G,

$$|G| = \sum [G : C(a)]$$

where the sum runs over one element a from each conjugacy class of G.

Proof of Corollary.

$$\begin{aligned} |G| &= \sum_a |\mathrm{cl}(a)| \qquad \text{(sum runs over)} \\ &= \sum [G : C(a)] \end{aligned}$$

□

Theorem 24.2
Let G be a finite group such that $|G| = p^n$ where $n \geq 1$. Then $Z(G)$ has more than one element.

Proof of Theorem 24.2. Notice that $a \in Z(G) \iff \mathrm{cl}(a) = \{a\}$

Thus we have that

$$|G| = |Z(G)| + \sum [G : C(a)] = \sum |\mathrm{cl}(a)|$$

where the above sum runs over representatives of all conjugacy classes with more than one element

$$\begin{aligned} & [G : C(a)] = \frac{|G|}{|C(a)|} = p^k \text{ with } k \geq 1 \\ \implies & |Z(G)| = |G| - \sum [G : C(a)] = p^n - \sum p^k \text{ divisible by p} \\ \implies & |Z(G)| \neq 1 \end{aligned}$$

□

Corollary 24.3
If $|G| = p^2$ where p prime, then G abelian.

Proof of Corollary. $|Z(G)| \,\big|\, p^2$ and $|Z(G)| \neq 1$ (by Thm) $\implies |Z(G)| = p$ or p^2

$$\begin{aligned} \text{If } |Z(G)| = p^2 &\implies G = Z(G) \\ &\implies G \text{ abelian} \\ \text{If } |Z(G)| = p &\implies |G/Z(G)| = p \\ &\implies G/Z(G) \text{ cyclic} \\ &\implies G \text{ abelian} \implies Z(G) = G \quad (\Rightarrow\!\Leftarrow) \end{aligned}$$

□

Theorem 24.3 (Sylow's First Theorem)
Let G be a finite group and let p be a prime. If $p^k \,\big|\, |G|$ then G has at least one subgroup of order p^k.

Proof of Sylow's First Theorem. Use induction on $|G|$. When $|G| = 1$ it is trivial.

Assume the statement holds for all groups or order less than $|G|$.

If $H < G$ and $p^k \mid |H|$ then we are done by induction.

Assume p^k does not divide the order of any proper subgroup of G.

Consider $|G| = |Z(G)| + \sum [G : C(a)]$, where we sum over a representative of each conjugacy class $\mathrm{cl}(a)$ with $a \notin Z(G)$

By FTFAG (or Cauchy's theorem for abelian groups), $\exists x \in Z(G)$ with $|x| = p$

Since $x \in Z(G) \implies \langle x \rangle \lhd Z(G) \lhd G \implies \langle x \rangle \lhd G$

So, we can formulate $G/\langle x \rangle$

Since $|G/\langle x \rangle| = \frac{|G|}{|\langle x \rangle|} = \frac{|G|}{p} \implies p^{k-1} \mid |G/\langle G \rangle|$

Note that ($G \to G/\langle x \rangle$ is p-to-1)

Then by induction $\exists$subgroup of order p^{k-1} of $G/\langle x \rangle$ and such a subgroup has form $H/\langle x \rangle$ where $H \leq G$.

But now $|H|/\langle x \rangle = p^{k-1} and |\langle x \rangle| = p$ so $|H| = p^k$ ($\Rightarrow\Leftarrow$). ☐

Lecture 29 (11/01)

Definition 4 (Sylow p-subgroup)
Let G be a finite group and let p be a prime. A subgroup $H \leq G$ is called a *Sylow p-subgroup* of G if $|H| = p^k$ and $p^k \mid |G|$ but $p^{k+1} \nmid |G|$.

Example 14
$|G| = 2^3 \cdot 3^2 \cdot 5^4 \cdot 7 \implies \exists$ subgroups of order:

2, 4, 8 (Sylow 2-gp), 3, 9 (sylow 3-gp), 5, 25, 125 (sylow 5-gp), 7 (sylow 7-sgp).

Corollary 24.4 (Cauchy's Thm)
Let G be a finite group and let p be a prime. If $p \mid |G|$ then G has an element of order p.

Corollary 24.5
The converse of Lagrange's theorem holds for finite abelian groups and all finite gps of prime power order (if $|G| = p^k$, then for any $m \leq k$ $\exists H \leq G$ st $|H| = p^m$).

Fact 1
A_4 does not have any subgroup of order 6 ($|A_4| = 12 = 2^2 \cdot 3$)

Theorem 24.4 (Sylow's Second Theorem)
Let G be a finite group and let p be a prime. If $H \leq G$ and $|H| = p^k$ then H is contained in some Sylow p-subgroup of G.

Theorem 24.5 (Sylow's Third Theorem)
Let $|G| = p^k m$ where p prime and $p \nmid m$. Then the number of Sylow p-subgroups of G is congruent to 1 modulo p and divides m. Furthermore, any two Sylow p-subgroups of G are conjugate to each other.

Corollary 24.6
A Sylow p-subgroup of a finite group G is normal iff it is the only SPSGP of G.

Example 15
$S_3 = \{(1), (12), (13), (23), (123), (132)\}$

Sylow 2-sgp: $\{(1), (12)\}, \{(1), (13)\}, \{(1), (23)\}$

$(13)\{(1), (12)\}(13)^{-1} = \{(1), (23)\}$

$(23)\{(1), (12)\}(23)^{-1} = \{(1), (13)\}$

Sylow 3-sgp: $\{(1), (123), (132)\} \triangleleft S_3$

Example 16
Recall that the group $A_4 = \{\text{even permutations of } S_4\}$.

$|A_4| = |S_4|/2 = 12 = 2^2 \cdot 3$

Then $\{(1), (12)(34), (13)(24), (14)(23)\}$ is the unique Sylow 2-sgp of A_4 and is thus normal by cor.

Sylow p-subgroupof order 2: $\{(1), (12)(34)\}, \{(1), (13)(24)\}, \{(1), (14)(23)\}$

Theorem 24.6 (24.6)
$|G| = pq$, p, q prime st $p < q$ and $p \nmid (q-1)$. Then G is cyclic and $G \cong \mathbb{Z}_{pq}$.

Example 17
Any finite group of order 15 is cyclic (i.e. $\cong \mathbb{Z}_{15}$)

Proof of Theorem 24.6. Let H be the Sylow p-subgroupof G. Let K be the Sylow q-subgroup of G.

By Sylow's Third Theorem, # of Sylow p-subgroups of G divides q and $\equiv 1 \pmod{p}$.

Since $p \nmid (q-1)$, H is the only Sylow p-subgroupof G.

Similarly K is the only Sylow q-subgroup of G.

Thus $H \triangleleft G$ and $K \triangleleft G$.

Let $H = \langle x \rangle$ and $K = \langle y \rangle$.

$\implies |x| = p$, $|y| = q$, $H \cap K = \{e\}$, $|HK| = \frac{|H||K|}{|H \cap K|} = pq = |G|$.

$\implies H \cap K = \{e\}$ and $HK = G$

$\implies G = H \times K \cong \mathbb{Z}_p \oplus \mathbb{Z}_q \cong \mathbb{Z}_{pq}$ $\square$

Example 18
Determine G with $|G| = 99 = 3^2 \cdot 11$.

H_3: Sylow 3-sgp $\qquad$ H_{11}: Sylow 11-sgp of G

$$\begin{aligned}
n_3 = \#\text{ of Sylow 3-sgps} &\implies n_3 \mid 11 \text{ and } n_3 \equiv 1 \bmod 3 \\
&\implies n_3 = 1 \implies H_3 \lhd G \\
n_{11} = \#\text{ of Sylow 11-sgps} &\implies n_{11} \mid 9 \text{ and } n_{11} \equiv 1 \bmod 11 \\
&\implies n_{11} = 1 \implies H_{11} \lhd G \\
H_3 \cap H_{11} = \{e\} &\implies |H_3H_{11}| = \frac{|H_3|\,|H_{11}|}{|H_3 \cap H_{11}|} = 99 \implies H_3H_{11} = G
\end{aligned}$$

So, we have $H_3 \lhd G$, $H_{11} \lhd G$, $H_3 \cap H_{11} = \{e\}$, $H_3H_{11} = G$

$\implies G = H_3 \times H_{11} \cong H_3 \oplus H_{11}$

$$|H_{11}| = 11 \implies H_{11} \cong \mathbb{Z}_{11} \qquad |H_3| = 3^2 = 9 \implies H_3 \cong \mathbb{Z}_9 \text{ or } \mathbb{Z}_3 \oplus \mathbb{Z}_3$$

$\implies G \cong \mathbb{Z}_9 \oplus \mathbb{Z}_{11}$ or $G \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{11}$

Lecture 30 (11/04)

Recall

1. If G is a finite group of permutations on a set S and $i \in S$, then

$$\begin{aligned}
\text{orb}_G(i) &= \{\phi(i) \mid \phi \in G\} \subseteq S \\
\text{stab}_G(i) &= \{\phi \in G \mid \phi(i) = i\} \leq G \\
[G : \text{stab}_G(i)] &= |\text{orb}_G(i)|
\end{aligned}$$

2. (N/C Theorem) Let $H \leq G$. Recall the *normalizer of H in G* and the *centralizer of H in G*,

$$\begin{aligned}
N_G(H) &= \{x \in G \mid xHx^{-1} = H\} \\
C_G(H) &= \{x \in G \mid xhx^{-1} \in H,\ \forall h \in H\} \\
N_G(H) \;/\; C_G(H) &\;\leq \text{Aut}(H)
\end{aligned}$$

Proof of Sylow's Second Theorem. Let $H \leq G$, $|H| = p^k$, $p^k \mid |G|$

Let K be a Sylow p-subgroup of G.

Let $C = \{K_1 = K, K_2, \ldots, K_n\}$ be the set of conjugates of K by elements of G
(i.e. $K_i = g_iKg_i^{-1}$ for some $g_i \in G$)

Then $|C| = [G : N_G(K)]$

Then the mapping $G \to C$ where $g \mapsto gKg^{-1}$ is surjective.

$$\begin{aligned}
g \text{ and } h \text{ have the same image} &\iff gKg^{-1} = hKh^{-1} \\
&\iff (h^{-1}g)K(h^{-1}g)^{-1} = K \\
&\iff h^{-1}g \in N_G(K) \\
&\iff gN_g(K) = hN_G(K) \\
&\iff \text{1-1 correspondence between elements of } C \text{ and left coests of } N_G(K) \\
&\implies |C| = [G : N_G(K)]
\end{aligned}$$

Consider the action of H on C given by h acts on K_i by hK_ih^{-1}

Then $|\text{orb}_H(K_i)| = [H : \text{stab}_H(K_i)]$ is a power of p and

$$\begin{aligned}
|\text{orb}_H(K_i)| = 1 &\iff \text{stab}_H(K_i) = H \\
&\iff H \leq N_G(K_i)
\end{aligned}$$

Claim 3. $H \leq N_G(K_i) \iff H \leq K_i$

Proof of claim. "$\Longleftarrow$" obvious.

"$\Longrightarrow$" $\forall x \in H$, $|x|$ is a power of p (since $|x| \mid |H| = p^k$)

$\forall y \in N_G(K_i) \leq K_i \quad |yK_i| \mid |\ N_G(K_i)\ /\ K_i\ |$

But $|\ N_G\ /\ K_i\ | = \frac{|N_G(K_i)|}{|K_i|} \mid \frac{|G|}{|K_i|}$($\leftarrow$ this is rel prime to p since K_i = sylow p-sgp

$\implies p \nmid |yK_i|$ and $|yK_i| \neq 1$

$\implies |y|$ is not a power of p because $|yK_i| \mid |y|$ ■

Summing up, we see that if $|\text{orb}_H(K_i)| = 1$ then $H \leq K_i$.

Now, $|C| = [G : N_G(K)] = \frac{|G|}{|N_G(K_i)|} = \underbrace{\frac{\frac{|G|}{|K|}}{\frac{|N_G(K_i)|}{|K|}}}_{\text{this is not divisible by } p}.$

If no orbit of C under H has size 1, then p divides the size of each orbit

then p divides $|C|$ ($\Rightarrow\!\Leftarrow$)
($\implies \exists K_i$ s.t. $|\text{orb}_H(K_i)| = 1$) □

Proof of Sylow's Third Theorem. Let $|G| = p^k m$ and $K \leq G$ be a Sylow p-subgroup
Let $C = \{K_1 = K, K_2, \ldots, K_n\}$ be the set of conjugates of K in G.

Consider the action of K on G by conjugation.

Then

- $|\text{orb}_K(K_i)| = [K : \text{stab}_K(K_i)]$ divides $|K| = p^k$
- $$\begin{aligned} |\text{orb}_K(K_i)| = 1 &\iff \text{stab}_K(K_1) = K \\ &\iff K \leq N_G(K_i) \overset{claim}{\iff} K \leq K_i \iff K = K_i \end{aligned}$$

  $\implies n = |C|$ is equal to 1 modulo p

  RTS that any Sylow p-subgroupis one of the K_i (i.e. conjugate to K)

  If K' is another Sylow p-subgroupof G and $K' \notin C$, then consider the action of K' on C by conjugation.

  Then the size of each orbit is greater than 1 (since $\text{orb}_{K'}(K_i) = 1 \iff K' = K_i$ which is impossible)

  $\implies$ summing up, $|C| \equiv 0 \bmod p$ contradicting $|C| \equiv 1 \bmod p$

  $\implies$ any Sylow p-subgroupis a conjugate of K we started with.

  Finally, $|C| = \frac{|G|}{|N_G(K)|}$ divides $|G| = p^r m$ and $|C| \equiv 1 \bmod p$.

  Since $\gcd(p, m) = 1 \implies |C| \mid m$

□

Lecture 31 (11/06)

Applications of Sylow's Theorems

Example 19
Any group of order 66 contains a subgroup isomorphic to $\mathbb{Z}_{33}$ $(66 = 2 \cdot 3 \cdot 11)$

H_p = Sylow p-sgp, $n_p = \#$ of Sylow p-subgroups

Then $n_{11} \mid 6$ and $n_{11} \equiv 1 \mod 11$ (by Sylow's Theorem)

$\implies n_{11} \implies H_{11}$ is a normal subgroup

Now, $H_3 H_{11} = H_{11} H_3$ is a subgroup (since H_{11} is normal)

$H_3 \cap H_{11} = \{e\} \implies |H_3 H_{11}| = \frac{|H_3||H_{11}|}{|H_3 \cap H_{11}|} = 3 \cdot 11 = 33 \implies H_3 H_{11}$ is a subgroup of order 33. $\square$

Note 2
Any group of order 33 is isomorphic to $\mathbb{Z}_{33}$ (pq such that $p \leq q$ and $p \nmid (q-1)$)

In fact, we can completely classify all groups of order 66 (Example 7 on pg 420)

There are exactly 4 such groups (up to $\cong$)

- $\mathbb{Z}_{66}$ $\quad \langle 2 \rangle \leq \mathbb{Z}_{66}$ subgroup of order 33
- D_{33} $\quad \{\text{rotations}\} \leq D_{33}$ " "
- $D_{11} \oplus \mathbb{Z}_3$ $\quad \mathbb{Z}_{11} \oplus \mathbb{Z}_3 \leq D_{11} \oplus \mathbb{Z}_3$ " "
- $\mathbb{Z}_{11} \oplus D_3$ $\quad \mathbb{Z}_{11} \oplus \mathbb{Z}_3 \leq \mathbb{Z}_{11} \oplus D_3$ " "

Example 20
Let G be a group of order $20 = 2^2 \cdot 5$ that is not abelian, then G has 5 Sylow 2-sgps.

By Sylow's Theorem, $n_5 \mid 4$ and $n_5 \equiv 1 \mod 5 \implies n_5 = 1$

$n_2 \mid 5$ and $n_2 \equiv 1 \mod 2 \implies n_2 = 1$ or $n_2 = 5$

Suppose $n_2 = 1$, then $H_2 \lhd G$ and $H_5 \lhd G$

Also $H_2 \cap H_5 = \{e\}$ $\quad |H_2 H_5| = \frac{|H_2||H_5|}{|H_2 \cap H_5|} = 4 \cdot 5 = 20$

$$\left.\begin{array}{l} \implies G = H_2 \times H_5 \cong H_2 \oplus H_5 \\ \text{but } |H_2| = 4 \implies H_2 \cong \mathbb{Z}_4 \text{ or } \mathbb{Z}_2 \oplus \mathbb{Z}_2 \\ |H_5| = 5 \implies H_5 \cong \mathbb{Z}_5 \end{array}\right\} \implies \underbrace{G = \text{ abelian}}_{(\Rightarrow\Leftarrow)}$$

Therefore $n_2 = 5$.

Example 21
Classify groups of order $255 = 3 \cdot 5 \cdot 17$

$n_{17} \mid 15$ and $n_{17} \equiv 1 \bmod 17$ (Sylow's Theorem)

$\implies n_{17} = 1 \implies \mathbb{Z}_{17} \cong H_{17} \lhd G \implies N(H_{17}) = G$

By $N \,/\, C$ Theorem,

$$\begin{aligned} & N(H_{17}) \,/\, C(H_{17}) \leq \mathrm{Aut}(H_{17}) \\ & \left| G \,/\, C(H_{17}) \right| \,\Big|\, |\mathrm{Aut}(H_{17})| = |U(17)| = 16 \\ & \left| G \,/\, C(H_{17}) \right| \,\Big|\, |G| = 255 = 3 \cdot 5 \cdot 7 \\ \implies & \left| G \,/\, C(H_{17}) \right| \,\Big|\, \gcd(16, 255) = 1 \\ \implies & C(H_{17}) = G \text{ i.e. elts of } G \text{ comm. with any elt in } H_{17} \\ \implies & H_{17} \leq Z(G) \implies 17 \,\Big|\, |Z(G)| \end{aligned}$$

Therefore $|Z(G)| = 17,\ 3 \cdot 17,\ 5 \cdot 17,\ 3 \cdot 5 \cdot 17$ $\big(\Longleftarrow |Z(G)| \,\big|\, 255 \text{ and } 17 \,\big|\, |Z(G)|\big)$.
i.e., $\left| G \,/\, Z(G) \right| = 15,\ 5,\ 3,$ or 1

But any group of order 15, 5, 3, or 1 is cyclic ($15 = pq$ such that $p \leq q$ and $p \nmid (q-1)$).

Recall if $G \,/\, Z(G)$ cyclic, then G abelian, so G is abelian.

Now by FTFAG, $G \cong \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{17} (\cong \mathbb{Z}_{255})$.

Lecture 32 (11/12)

12 Introduction to Rings

12.1 Motivation & Definition

Definition 5 (Ring)
A ring R is a set with two binary operations: $a + b$ and $a \cdot b = ab$ such that for all $a, b, c \in R$,

1. $a + b = b + a$
2. $(a + b) + c = a + (b + c)$
3. $\exists$ an additive identity 0, $a + 0 = a$
4. $\exists$ an element $-a \in R$ such that $a + (-a) = 0$
5. $(ab)c = a(bc)$
6. $a(b + c) = ab + ac$

   $(b + c)a = ba + ca$

So a ring is an abelian group under addition, and also has an associative multiplication that is left and right distributive over addition.

- The multiplication need not be commutative. When it is, we say the ring is commutative.
- A unity (or identity): a nonzero element that is an identity under multiplication.
- unit: a nonzero element of a commutative ring with identity that has a multiplicative inverse.
- In R, $a \mid b$ if $\exists c \in R$ such that $b = ac$.
- $n \in \mathbb{Z}_{>0}$, $na = \underbrace{a + a + \cdots + a}_{\text{n times}}$

12.2 Examples of Rings

Example 22
$(\mathbb{Z}, +\times)$ is a commutative ring with identity and units $= \pm 1$

Example 23
$(\mathbb{Z}_n, +\times)$ is a commutative ring with identity and units $= U(n)$

Example 24
$(\mathbb{Z}[x], +\times)$ is a commutative ring with identity

Example 25
$(\mathbb{M}_2[\mathbb{Z}], +\times)$ is a non-commutative ring with identity

Example 26
$(2\mathbb{Z} = \{\text{even integers}\}, +\times)$ is a comm ring without identity

Example 27
$(\{\text{continuous functions on } \mathbb{R}, +\times\})$ is a comm ring with identity $f(x) = 1$

Example 28
$(\{\text{continuous functions on } \mathbb{R} \text{ whose graphs pass through } (1, 0), +\times\})$ is a comm ring without identity

Note $f(1) = 0$, $g(1) = 0$, $f + g, fg$

Definition 6 (Direct sum of rings)
Let $R_1, R_2, \ldots, R_n$ be rings. Construct

$$R_1 \oplus R_2 \oplus \cdots \oplus R_n = \{(r_1, r_2, \ldots, r_n) \mid r_i \in R_i\}$$

endowed with component-wise addition and multiplication. This is called the direct sum of $R_1, R_2, \ldots, R_n$.

12.3 Properties of Rings

Theorem 12.1 (Rules of Multiplication)
For all $a, b, c \in R$,

1. $a \cdot 0 = 0 \cdot a = 0$
2. $a(-b) = (-a)b = -(ab)$
3. $(-a)(-b) = ab$
4. $a(b - c) = ab - ac$
   $(b - c)a = ba - ca$
5. $(-1)a = -a$
6. $(-1)(-1) = 1$

Note 3
Properties 5 and 6 only hold if R has an identity 1

Proof of property 1. Clearly $0+a0 = a0 = a(0+0) = a0+a0$, so by cancellation $0 = a0$ and similarly $0a = 0$ □

Theorem 12.2 (Uniqueness of the Unity and Inverses)
If a ring R has a unity, it is unique. If a ring element has a multiplicative inverse, it is unique.

Proof. 1, 1' $\implies$ 1=1·1' = 1'

$a \quad ab = ba = 1$

$ac = ca = 1$

$c = c \cdot 1 = c(ab) = (ca)b = 1 \cdot b = b$ □

Warning
In general, $ab = ac \;\not\Longrightarrow\; b = c$ (cancellation rule does not hold in general for multiplication).

Example 29
In $\mathbb{Z}_6$, notice $2 \cdot 3 = 0 = 3 \cdot 0$ but $2 \neq 0$

12.4 Subrings

Definition 7 (Subring)
A subset $S \subseteq R$ is a subring of R if S is itself a ring with the operations of R

Theorem 12.3 (Subring Test)
A nonempty subset S of a ring R is a subring if S is closed under sutraction and multiplication.

i.e. if $a, b \in S$ then $a - b \in S$ and $ab \in S$

Example 30
$\{0\}$ and R will always be subrings of any ring R.

Example 31
$\{0, 2, 4\} \subseteq \mathbb{Z}_6$ is a subring

1 is the identity in $\mathbb{Z}_6$

4 is the identity in $\{0, 2, 4\}$ $(0 \cdot 4 = 0,\ 2 \cdot 4 = 2,\ 4 \cdot 4 = 4)$

Example 32
$n\mathbb{Z} = \{0, \pm n, \pm 2n, \pm 3n, \ldots\}$ is a subring of $\mathbb{Z}$ that does not have any identity (if $n \neq 1$).