Algebra MATH-310

Lecture 7

Anna Lachowska

November ~~5~~ 4, 2024

Written assignment: 18 nov → 25 nov

Plan of the course

1. Integers: 1 lecture
2. Groups: 6 lectures
3. Rings and fields: 5 lectures
4. Review: 1 lecture

Today: Groups: lecture 6 → the last on groups

(a) Groups: general picture

(b) If a prime p divides $|G|$, then there exists an element of order p in G

(c) Classification of simple finite abelian groups

(d) Direct product of groups

(e) Classification of finite abelian groups

(f) Elementary divisors and invariant factors: examples

Finite groups

	Abelian	Non-abelian
Definition	$ab = ba \ \forall a, b \in G$	$\exists a, b \in G : \quad ab \neq ba$
Normal subgroups	All subgroups	$H \trianglelefteq G : \ gHg^{-1} \in H \ \forall g \in G$
Conjugacy classes	$\lvert C_i \rvert = 1 \ \ \forall C_i$	$\exists C_i : \ \lvert C_i \rvert > 1$
Class equation	$\lvert G \rvert = \lvert Z(G) \rvert$	$\lvert G \rvert = \underbrace{\lvert Z(G) \rvert}_{\text{center}} + \sum_{i=1}^{r} \lvert C_i \rvert,$ $\lvert C_i \rvert > 1$
Examples	Cyclic groups C_n Any others?	Symmetric group S_n Dihedral group D_n

Cauchy's theorem

Theorem

Let G be a finite abelian group, and p a prime dividing $|G|$. Then G contains an element of order p.

Proof: Let G be the smallest counter-example: $|G|$ is minimal s.t. $\nexists$ elt of order p in G, where p is a prime, p divides $|G|$.

Let $g \in G \Rightarrow$ order(g) is not divisible by p (if $g^{kp} = 1 \Rightarrow (g^k)^p = 1$)

$\langle g \rangle \subset G$ subgp, $|\langle g \rangle| = \text{order}(g) \Rightarrow |G/\langle g \rangle| = |G|/\langle g \rangle < |G|$

$\Rightarrow p$ divides $|G/\langle g \rangle|$ and $G/\langle g \rangle$ contains an elt h of order p.

$\Rightarrow h^p \in \langle g \rangle \Rightarrow h^p = g^s$, let k be the order of $g^s \Rightarrow$

$(h^p)^k = (g^s)^k = 1 \Rightarrow (h^k)^p = 1 \Rightarrow h^k$ is the elt of order p.

$\square$

Cauchy's theorem

Non-abelian case

Cauchy's theorem holds for non-abelian finite groups as well.

p divides $|G|$ $\Rightarrow$ $\exists$ an elt $g \in G$ s.t. the order of g is equal to p.

a prime

Easier: use the class equation and the abelian case [PS7].

Classification of finite abelian simple groups

Definition

A group G is simple if G has no proper nontrivial normal subgroups.

$\neq G$ $\quad \neq \{1\}$ $\quad H \triangleleft G$, $gHg^{-1} \in H$

Proposition

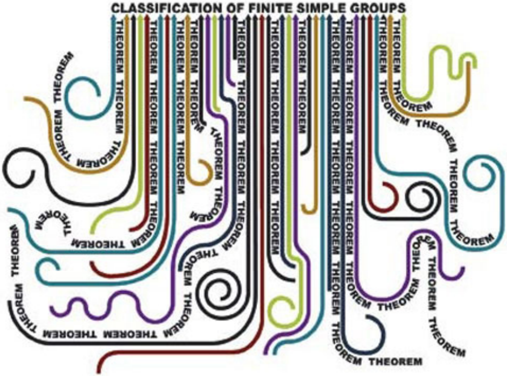
If G is a simple finite abelian group, then G is isomorphic to a cyclic group C_p of prime order.

Proof: $|G| = p_1^{n_1} \cdots p_k^{n_k}$ prime factorization $\Rightarrow$ by Cauchy's thm
$\exists$ an elt of order p_1 in G. $: g \in G :$ $\langle g \rangle \subset G$, normal (G is abelian)
$\langle g \rangle \subset G$ not proper $\Leftrightarrow$ $|G| = |p_1|$ $\Leftrightarrow$ G is simple.
For G to be simple it has to be of order $= p_1$ $\Rightarrow$
$G = \langle g \rangle \simeq C_{p_1}$ $\blacksquare$

Classification of finite non-abelian simple groups (2012)

180 years of work by more than 30 mathematicians.

Answer: 18 infinite series and 27 exceptional groups. The order of the biggest exceptional simple group, The Monster, is about $8 \cdot 10^{53}$.



Our goal today: classification of all finite abelian groups

Direct product of groups $(AICC\ \mathrm{II})$

Definition

Let G, H be groups. The direct product $G \times H$ is the set of pairs $G \times H = \{(g, h),\ g \in G, h \in H\}$ with multiplication $(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$, the neutral element $(1_G, 1_H)$ and the inverse $(g^{-1}, h^{-1})(g, h) = (1_G, 1_H)$.

Example: $G = C_2 \times C_3. = \{(g,h) : g \in C_2, h \in C_3\}$ $C_2 = \langle a \mid a^2 = 1 \rangle$, $C_3 = \langle b \mid b^3 = 1 \rangle$

$\{(1,1), (1,b), (1,b^2), (a,1), (a,b), (a,b^2)\} = C_2 \times C_3$. Let $t = (a,b)$

$\Rightarrow t^2 = (1, b^2)$, $t^3 = (a, 1)$, $t^4 = (1, b)$, $t^5 = (a, b^2)$, $t^6 = (1, 1)$

$\Rightarrow t \in C_2 \times C_3$ has order 6. ; $|C_2 \times C_3| = 6$

$\Rightarrow C_2 \times C_3 \simeq C_6$ is cyclic

Question: Is $C_n \times C_m \simeq C_{nm}$ always?

Direct product of groups

Example: $G = \underset{a^2=1}{\underset{a}{C_2}} \times \underset{b^2=1}{\underset{b}{C_2}}$. $= \{(1,1), (1,b), (a,1), (a,b)\} \not\cong C_4$

each elt has order 2:

$(1,b)(1,b) = (1,1)$ etc.

$\Rightarrow C_2 \times C_2$ does not have an elt of order 4.

$\Rightarrow C_2 \times C_2 \not\cong C_4$.

Remark

Suppose $(a, b) \in C_n \times C_m$ such that $o(a) = n$, $o(b) = m$. then $(a, b)^s = (a^s, b^s) = (1, 1)$ implies $o(a)$ divides s and $o(b)$ divides s. Therefore, the order of (a, b) is $\mathrm{lcm}(o(a), o(b)) = \mathrm{lcm}(n, m)$.

Direct product of cyclic groups

Proposition

$C_n \times C_m \simeq C_{nm}$ if and only if $\gcd(n, m) = 1$.

Proof: PS 7. use the remark above.

Corollary

Let C_n be a cyclic group such that $n = p_1^{k_1} \overbrace{p_2^{k_2} \dots p_r^{k_r}}^{m}$ is the prime factorization of n. Then $C_n \simeq C_{p_1^{k_1}} \times C_{p_2^{k_2}} \times \dots \times C_{p_r^{k_r}}$.

Proof: $C_n \simeq C_{p_1^{k_1}} \times C_m$, $m = p_2^{k_2} \dots p_r^{k_r}$ by Proposition, because $\gcd(p_1^{k}, m) = 1$

Repeat with C_m, and so on .....

$\Rightarrow$ get the decomposition $\square$

Properties of the direct product of groups

$|G \times H| = |G| \cdot |H|$

1. $G \times H \simeq H \times G$, $|G \times H| = |G| \cdot |H|$. $\varphi : (g,h) \to (h,g)$ isomorphism

2. $H \subset G \times H$, $G \subset G \times H$ are subgroups. $\{(1,h), h \in H\} \simeq H \subset G$

3. $G \times H$ is abelian if and only if G and H are abelian.

4. If $H, K \subset G$ are subgroups such that
   (a) $H \cap K = \{1\}$
   (b) $\forall h \in H, \forall k \in K$, $hk = kh$
   (c) $HK = \{hk\}_{h \in H, k \in K} = G$

   Then $G \simeq H \times K$. The isomorphism is given by $\phi : H \times K \to G$, $\phi(h,k) = hk$.

   See groups.pdf on Moodle

Classification of finite abelian groups

Theorem

Let G be a finite abelian group. Then G is isomorphic to a direct product of cyclic groups of prime power orders

$$G \simeq C_{p_1^{n_1}} \times C_{p_2^{n_2}} \times \ldots \times C_{p_m^{n_m}},$$

where $|G| = p_1^{n_1} p_2^{n_2} \ldots p_m^{n_m}$. Here $\{p_1, p_2, \ldots p_m\}$ are primes, not necessarily distinct, and $n_1, \ldots n_m \geq 1$.
This presentation if unique up to the order of factors. The numbers $(p_1^{n_1}, p_2^{n_2}, \ldots p_m^{n_m})$ are called the elementary divisors of G.

Examples:

$C_3 \times C_2 \simeq C_6$; $C_2 \times C_2 \simeq G$, $|G| = 4$

cyclic

abelian, not cyclic

Proof of the classification theorem

Generators and relations $G = \langle g_1, \ldots g_k \mid R_1, \ldots R_\ell \rangle$

$$R_1 = g_1^{n_{11}} g_2^{n_{12}} \ldots g_k^{n_{1k}} = 1$$
$$R_2 = g_1^{n_{21}} g_2^{n_{22}} \ldots g_k^{n_{2k}} = 1$$
$$\ldots$$
$$R_\ell = g_1^{n_{l1}} g_2^{n_{l2}} \ldots g_k^{n_{lk}} = 1$$

They can be encoded in a rectangular matrix

$$\begin{pmatrix} n_{11} & n_{12} & \ldots & \ldots & n_{1k} \\ n_{21} & n_{22} & \ldots & & \\ n_{31} & n_{32} & \ldots & & \\ & & & & \\ & & & & \end{pmatrix}$$

ℓ rows
k columns

Which operations on the matrix do not change the group G?

Operations on the matrix without changing the group

1. Adding an integer multiple of one row to another row.

Ex $\begin{pmatrix} 3 & 1 \\ 1 & -2 \end{pmatrix} \Rightarrow$ row 1 + 2·(row 2) $\Rightarrow \begin{pmatrix} 5 & -3 \\ 1 & -2 \end{pmatrix}$

Relations: $\begin{cases} g^3 h = 1 \\ g h^{-2} = 1 \end{cases} \Rightarrow \begin{matrix} g^3 h \cdot (g h^{-2})^2 = g^5 h^{-3} = 1 \\ g h^{-2} = 1 \end{matrix} = \begin{cases} g^5 h^{-3} = 1 \\ g h^{-2} = 1 \end{cases}$ define the same group

2. Adding integer multiple of one column to another column.

$g^n h^m = 1$. Replace generators $(g, h) \to (gh^{-3}, h)$ $\Rightarrow$ the relation becomes

$\underbrace{(gh^{-3})}_{f}{}^{n} \cdot \underbrace{h}_{h}{}^{m+3n} = g^n h^{-3n} h^m h^{3n} = g^n h^m = 1$

In the new generators $f^n h^{m+3n} = 1$ define the same group

column 2 + 3 column 1 : $(n, m) \to (n, m+3n)$

3. Swapping two columns or swapping two rows.

$\longleftrightarrow$ reordering generators and relations

Operations on the matrix without changing the group

Applying these operations, we can get $n_{11} = \gcd$(elements of the first column and first row). Then by column and row operations we get

$$\begin{pmatrix} n_{11} & 0 & 0 & \dots & 0 \\ 0 & n_{22} & \dots & & \\ 0 & n_{32} & \dots & & \\ 0 & & & & \\ 0 & & & & \end{pmatrix}$$

Repeating with the smaller matrix, we get the diagonal matrix

$$\begin{pmatrix} n_{11} & 0 & 0 & \dots & 0 \\ 0 & n_{22} & \dots & & \\ 0 & 0 & n_{33} & & \\ 0 & & & & \\ 0 & & & & \end{pmatrix}$$

This matrix defines the same group:

$$G = \langle g_1, g_2, \dots g_r \mid g_1^{n_{11}} = 1, g_2^{n_{22}} = 1, \dots g_r^{n_{rr}} = 1 \rangle.$$

The classification theorem: end of the proof

We have $G = \langle g_1, g_2, \dots g_r \mid g_1^{n_{11}} = 1, g_2^{n_{22}} = 1, \dots g_r^{n_{rr}} = 1 \rangle$.

$\Rightarrow$ $G_i = \langle g_i \rangle$ are cyclic subgroups ; $\langle g_i \rangle \cap \langle g_j \rangle = 1$

$g_i g_j = g_j g_i$ G abelian

$\Rightarrow$ By property (4) of the direct products

$G \simeq C_{n_{11}} \times C_{n_{22}} \times \dots \times C_{n_{kk}}$

By Proposition above each $C_{n_{11}} \simeq C_{p_1^{a_1}} \times C_{p_2^{a_2}} \dots \times C_{p_r^{a_r}}$

Finally, $G \simeq$

$$G \simeq C_{p_1^{n_1}} \times C_{p_2^{n_2}} \times \ldots \times C_{p_m^{n_m}},$$

a direct product of cyclic groups of prime power orders (not necessarily distinct primes).

Corollary: Structure of abelian groups of prime power order

Corollary

Let G be an abelian group. If $|G| = p^n$, where p a prime, then $G \simeq C_{p^{i_1}} \times C_{p^{i_2}} \times \ldots \times C_{p^{i_k}}$ such that $i_1 + i_2 + \ldots + i_k = n$.
The set of abelian groups of order p^n is in bijection with the partitions of n: $n = i_1 + i_2 + \ldots + i_k$, such that $i_1 \geq i_2 \geq \ldots \geq i_k \geq 1$.

Example: $|G| = 8.$ $= 2^3$

Partitions of 3: (3), $(2,1)$ $(1,1,1)$

$\Rightarrow$ $G_1 \simeq C_{2^3}$ $\quad G_2 \simeq C_{2^2} \times C_2$ $\quad G_3 \simeq C_2 \times C_2 \times C_2$

(3) $\quad (2,1)$

Pairwise non-isomorphic because $C_n \times C_m \simeq C_{nm} \Leftrightarrow \gcd(n,m) = 1$

Another way to encode a finite abelian group

Theorem

A finite abelian group $G \simeq C_{d_1} \times C_{d_2} \times \ldots \times C_{d_n}$, where d_n divides d_{n-1}, d_{n_1} divides d_{n-2}, etc, d_2 divides d_1, and $|G| = d_1 d_2 \ldots d_n$. The numbers $(d_1, d_2, \ldots d_n)$ are called the invariant factors of G. They determine G uniquely.

$$\begin{matrix} p_1^{a_{11}} & p_1^{a_{12}} & p_1^{a_{13}} \\ p_2^{a_{21}} & p_2^{a_{22}} & \\ p_3^{a_{31}} & p_3^{a_{32}} & p_3^{a_{33}} \\ \shortparallel & \shortparallel & \shortparallel \\ d_1 & d_2 & d_3 \end{matrix}$$

$\leftarrow$ Elementary divisors of G

$a_{11} \geq a_{12} \geq a_{13}$

$a_{21} \geq a_{22}$

$a_{31} \geq a_{32} \geq a_{33}$

$\Rightarrow$ by construction $d_3 | d_2$, $d_2 | d_1$

$C_{d_1} \times C_{d_2} \times C_{d_3}$ $\Rightarrow$ invariant factors: (d_1, d_2, d_3).

Algorithm to classify all abelian groups of given order

1. Decompose $|G| = n = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$ (prime factorization).
2. Find partitions for each power $k_1, k_2, \dots k_n$.
3. For each partition of k_i, there is a unique group of order $p_i^{k_i}$:

$$k_i = a_1 + a_2 + \ldots + a_t \quad \Longrightarrow \quad C_{p_i^{a_1}} \times C_{p_i^{a_2}} \times \ldots \times C_{p_i^{a_t}}.$$

4. The possible groups of order n are the direct products of all possible groups of orders $p_i^{k_i}$. This gives a decomposition of G as a direct product of cyclic groups of prime power orders - the elementary divisors of G.
5. For each of the distinct primes p_i, write the obtained cyclic groups $C_{p_i^{n_i}}$ in the order of decreasing powers of p_i, different primes in different lines. Then in each column you will have cyclic groups of coprime orders, their direct product is a cyclic group. Thus you obtain cyclic groups of orders $(d_1, d_2, \dots d_n)$ and by construction $d_n | d_{n-1} | \dots | d_2 | d_1$. These are the invariant factors of G.

Classification of finite abelian groups: example

$|G| = 72 = 2^3 \cdot 3^2$ partitions: (3) $(2,1)$, $(1,1,1)$

(2) $(1,1)$

$p_1=2$	$C_{2^3}\times$	$C_{2^3}\times$	$C_{2^2}\times C_2\times$	$C_{2^2}\times C_2\times$	$C_2\times C_2\times C_2\times$	$C_2\times C_2\times C_2$
$p_2=3$	C_{3^2}	$C_3\times C_3$	C_{3^2}	$C_3\times C_3$	C_{3^2}	$C_3\times C_3$
	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
	C_{72}	$C_{24}\times C_3$	$C_{36}\times C_2$	$C_{12}\times C_6$	$C_{18}\times C_2\times C_2$	$C_6\times C_6\times C_2$

There are 6 non-isomorphic abelian groups of order 72.

The elementary divisors: $\{(2^3, 3^2), (2^3, 3, 3), (2^2, 2, 3^2), (2^2, 2, 3, 3), (2, 2, 2, 3^2), (2, 2, 2, 3, 3)\}$.

The invariant factors: $\{(72), (24, 3), (36, 2), (12, 6), (18, 2, 2), (6, 6, 2)\}$

For example: $C_4\times C_2\times C_9 \simeq C_{36}\times C_2 \simeq C_4\times C_{18}$

elementary divisors invariant factors neither: 4 does not divide 18 18 is not a prime power

Poll:

$225 = 3^2 \cdot 5^2$ $\quad$ $36 = 2^2 \cdot 3^2$

4 gps $\quad$ 4 gps

$C_n \times C_m \simeq C_{nm} \Leftrightarrow (n,m)$ coprime

Which of the statements below is false?

A: There is only one abelian group of order 105 $= 3^1 \cdot 5^1 \cdot 7^1$ True

B: If p a prime, then $C_{p^3} \times C_{p^5}$ is not isomorphic to C_{p^8} True

C: The number of abelian groups of orders 225 and 36 is the same True

D: If m divides n, then any abelian group of order n contains an element of order m. False

Counter-example: $|C_2 \times C_2| = 4$, 4 divides 4 but no elt of order 4 in $C_2 \times C_2$.

E: If a prime p divides $|G|$, then $C_p \subset G$

$\exists g \in G : g^p = 1 \Rightarrow \langle g \rangle \simeq C_p \subset G$