MATH 3030 ALGEBRA I

Lecture 2

Direct products

Def Let H, K be groups. Define a binary operation on $H \times K$ by
$$((h,k),(h',k')) \longmapsto (hh', kk')$$
Then $H \times K$ is a group, called the direct product of H and K

Prop Let $G = H \times K$. Then $\overline{H} = \{(h,e) \mid h \in H\} \triangleleft G$ and $G/\overline{H} \cong K$. Similarly, $G/\overline{K} \cong H$.

Pf: Consider the homomorphism
$$\pi_2 : G = H \times K \longrightarrow K$$
$$(h,k) \longmapsto k$$

π_2 is onto and $\mathrm{Ker}(\pi_2) = \overline{H}$, so $G/\overline{H} \cong K$. #

More generally, we have

Def/Prop Let $G_1, G_2, \ldots, G_n$ be groups. Define a binary operation on $\prod_{i=1}^n G_i \times \prod_{i=1}^n G_i \longrightarrow \prod_{i=1}^n G_i$ by

$$((a_1, a_2, \ldots, a_n), (b_1, b_2, \ldots, b_n)) \longmapsto (a_1 b_1, a_2 b_2, \ldots, a_n b_n)$$

Then $\prod_{i=1}^n G_i$ is a group, called the direct product of $G_1, G_2, \ldots, G_n$.

Rmk If G_i is abelian $\forall i$, then we call $\prod_{i=1}^n G_i$ the direct sum of G_i's and it's denoted by $\bigoplus_{i=1}^n G_i = G_1 \oplus G_2 \oplus \cdots \oplus G_n$. (cf. direct sum of vector spaces)

Prop Given $N_i \triangleleft G_i$ for $i = 1, \ldots, n$. Then $\prod_{i=1}^n N_i \triangleleft \prod_{i=1}^n G_i$ and

$$\prod_{i=1}^n G_i \Big/ \prod_{i=1}^n N_i \cong \prod_{i=1}^n (G_i / N_i)$$

(prove this!)

In general, given a normal subgroup $N \lhd \prod_{i=1}^{n} G_i$, the quotient $\left(\prod_{i=1}^{n} G_i\right)/N$ depends not just on the isomorphism class of N, but also on how N "sits" inside the product $\prod_{i=1}^{n} G_i$.

e.g. Consider $\mathbb{Z}_2 \times \mathbb{Z}_4$

Case 1: $N := \mathbb{Z}_2 \times \{0\} \lhd \mathbb{Z}_2 \times \mathbb{Z}_4 \implies \mathbb{Z}_2 \times \mathbb{Z}_4 / N \cong \mathbb{Z}_4$ (by above prop.)

Case 2: $N := \underset{\mathbb{Z}_2}{\underset{\cong}{\langle (1,2) \rangle}} \lhd \mathbb{Z}_2 \times \mathbb{Z}_4 \implies \mathbb{Z}_2 \times \mathbb{Z}_4 / N = \langle \overline{(1,1)} \rangle \cong \mathbb{Z}_4$

Case 3: $N := \underset{\mathbb{Z}_2}{\underset{\cong}{\langle (0,2) \rangle}} \lhd \mathbb{Z}_2 \times \mathbb{Z}_4 \implies \mathbb{Z}_2 \times \mathbb{Z}_4 / N \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ (by above prop.)

So $\mathbb{Z}_2 \times \mathbb{Z}_4$ quotient by a subgroup $\cong \mathbb{Z}_2$ can give different answers!

To see more such examples, let us study the structures of products of finite cyclic groups.

<u>Examples</u>. The Klein 4-group $V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. This is not cyclic.

- However, consider $\mathbb{Z}_2 \times \mathbb{Z}_3$. Then $|(1,1)| = 6 \Rightarrow \mathbb{Z}_2 \times \mathbb{Z}_3 = \langle (1,1) \rangle \cong \mathbb{Z}_6$, which is cyclic.

<u>Prop</u> Consider the group $\mathbb{Z}_m \times \mathbb{Z}_n$ $(m, n \in \mathbb{Z}_{\geq 1})$. The order of the element $(1,1) \in \mathbb{Z}_m \times \mathbb{Z}_n$ is given by $\mathrm{lcm}(m,n)$.

least common multiple

<u>Pf</u>: Let $k = |(1,1)|$. Then $k(1,1) = (0,0)$ in $\mathbb{Z}_m \times \mathbb{Z}_n$.

Hence, $m \mid k$ & $n \mid k$. So we have $\mathrm{lcm}(m,n) \mid k$.

On the other hand, we also have $\mathrm{lcm}(m,n) \cdot (1,1) = (0,0) \in \mathbb{Z}_m \times \mathbb{Z}_n$

$\Longrightarrow k \mid \mathrm{lcm}(m,n)$

As a result, $k = \mathrm{lcm}(m,n)$. #

Cor $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic iff m, n are relatively prime. (e.g. $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$)

Pf: ($\Leftarrow$): by the above proposition and the fact that $\gcd(m,n) \cdot \mathrm{lcm}(m,n) = mn$

($\Rightarrow$): $\forall (p,q) \in \mathbb{Z}_m \times \mathbb{Z}_n$, $\mathrm{lcm}(m,n) \cdot (p,q) = (0,0)$

$$\Longrightarrow \quad |(p,q)| \,\big|\, \mathrm{lcm}(m,n)$$

In particular, $|(p,q)| \leq \mathrm{lcm}(m,n)$

which is less than mn if m, n are not relatively prime. #

More generally, we have the following

Prop Let $(a_1, a_2, \ldots, a_n) \in \prod_{i=1}^{n} G_i$. Suppose that $|a_i| = r_i$. Then

$$|(a_1, a_2, \ldots, a_n)| = \mathrm{lcm}(r_1, r_2, \ldots, r_n)$$

Pf: Exercise. Similar to the proof of the above proposition. #

Structure of finitely generated abelian groups

Thm (Structure Theorem of f.g. abelian groups)

Every finitely generated abelian group G is isomorphic to a direct product (sum) of cyclic groups of the form

$$G \cong \underbrace{\mathbb{Z}^r}_{\text{free part } G_{\text{free}}} \times \underbrace{\mathbb{Z}_{p_1^{n_{11}}} \times \cdots \times \mathbb{Z}_{p_1^{n_{1\ell_1}}} \times \mathbb{Z}_{p_2^{n_{21}}} \times \cdots \times \mathbb{Z}_{p_2^{n_{2\ell_2}}} \times \cdots \times \mathbb{Z}_{p_k^{n_{k1}}} \times \cdots \times \mathbb{Z}_{p_k^{n_{k\ell_k}}}}_{\text{torsion part } G_{\text{tor}}} \quad \text{— } (*)$$

where $p_1 < p_2 < \cdots < p_k$ are primes and $\{n_{ij}\}_{j=1,\ldots,\ell_i}$ is a decreasing sequence of +ve integers.

The direct product is uniquely determined.

Pf: This is a corollary of the classification of fin. gen. modules over a PID. #

The nonnegative integer r is called the rank of G.
The prime powers $p_i^{n_{ij}}$ are called the elementary divisors of G.
Note that $|G_{tor}| = \prod_{i=1}^{k} \prod_{j=1}^{l_i} p_i^{n_{ij}}$.

Another way to formulate the isomorphism is as:

$$G \cong \mathbb{Z}^r \times \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_s} \quad \text{— } (**)$$

where $1 < d_1 | d_2 | \cdots | d_s$. This expression is also uniquely determined.
The +ve integers d_i are called invariant factors of G.
Note that $|G_{tor}| = d_1 d_2 \cdots d_s$.

The relation between (*) and (**) can be explained by the following diagram:

p_i increasing $\longrightarrow$

$$\begin{array}{r|c|c|c|c}
\hline
d_s = & p_1^{n_{11}} & p_2^{n_{21}} & p_3^{n_{31}} & \cdots \\
\hline
d_{s-1} = & p_1^{n_{12}} & p_2^{n_{22}} & p_3^{n_{32}} & \cdots \\
\hline
d_{s-2} = & p_1^{n_{13}} & p_2^{n_{23}} & p_3^{n_{33}} & \cdots \\
\hline
\vdots & \vdots & \vdots & \vdots &
\end{array}
\quad \Big\downarrow \; n_{ij} \text{ decreasing (as } j \text{ increases)}$$

Let $m = p_1^{n_1} \cdots p_k^{n_k}$ be a positive integer. Then the structure theorem a bijective correspondence

$$\left\{ \begin{array}{c} \text{partitions of } n_i \\ \text{for } i=1,\dots,k \end{array} \right\} \xleftrightarrow{1-1} \left\{ \begin{array}{c} \text{finite abelian groups} \\ \text{of order } m \end{array} \right\}$$

$$\begin{array}{c} n_i = n_{i1} + n_{i2} + \cdots + n_{i\ell_i} \\ n_{ij} > 0 \ \forall j \text{ for } i=1,\dots,n \end{array} \longleftrightarrow \prod_{i=1}^{k} \left(\mathbb{Z}_{p_i^{n_{i1}}} \times \mathbb{Z}_{p_i^{n_{i2}}} \times \cdots \times \mathbb{Z}_{p_i^{n_{i\ell_i}}} \right)$$

Examples ① For $m = 100 = 2^2 \cdot 5^2$, there are 4 isom. classes:

$\mathbb{Z}_{100}$, $\mathbb{Z}_2 \times \mathbb{Z}_{50}$, $\mathbb{Z}_5 \times \mathbb{Z}_{25}$, $\mathbb{Z}_{10} \times \mathbb{Z}_{10}$

$100 =$	2^2	5^2

$50 =$	2	5^2
$2 =$	2	

$25 =$	2^2	5
$5 =$		5

$10 =$	2	5
$10 =$	2	5

② For $m = 360 = 2^3 \cdot 3^2 \cdot 5$, there are 6 isom. classes:

$360 =$	2^3	3^2	5

$\mathbb{Z}_{360}$,

$180 =$	2^2	3^2	5
$2 =$	2		

$\mathbb{Z}_2 \times \mathbb{Z}_{180}$,

$120 =$	2^3	3	5
$3 =$		3	

$\mathbb{Z}_3 \times \mathbb{Z}_{120}$,

$90 =$	2	3^2	5
$2 =$	2		
$2 =$	2		

$\mathbb{Z}_2^2 \times \mathbb{Z}_{90}$,

$60 =$	2^2	3	5
$6 =$	2	3	

$\mathbb{Z}_6 \times \mathbb{Z}_{60}$,

$30 =$	2	3	5
$6 =$	2	3	
$2 =$	2		

$\mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_{30}$.

Cor Let F be a field and let $F^\times = F \setminus \{0\}$.
If $G < F^\times$ is a finite subgroup, then G is cyclic
In particular, $F^\times$ is cyclic if F is a finite field.

Pf: By the Str. Thm. of Finitely Gen. Abelian Groups,

$$G \cong \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_r}$$

where $d_i = p_i^{s_i}$ is a prime power for $i = 1, \ldots, r$.
Let $m := \operatorname{lcm}(d_1, \ldots, d_r) \leq |G|$. Then $\alpha^m = 1 \ \forall \alpha \in G$.
But the polynomial $x^m - 1$ has at most m roots.
So $|G| \leq m$, and we must have $m = |G| = d_1 \cdots d_r$.
Hence $p_1, \ldots, p_r$ are all distinct primes and $G \cong \mathbb{Z}_m$. #

e.g. $\mathbb{Z}_{13}^\times = \{1, 2, \ldots, 12\} = \langle 2 \rangle = \langle 6 \rangle = \langle 7 \rangle = \langle 11 \rangle$.

Computations of quotient groups

Rmks: • If G is cyclic, then G/N is cyclic. (Why?)
• If G is abelian, then G/N is abelian. (Why?)

e.g. Consider $N := \langle (2,3) \rangle \lhd \mathbb{Z}_4 \times \mathbb{Z}_6$.
We want to compute the quotient $\mathbb{Z}_4 \times \mathbb{Z}_6 / N$.
First of all, the order of the subgroup is $|(2,3)| = 2$.
Hence, $|\mathbb{Z}_4 \times \mathbb{Z}_6 / N| = 24/2 = 12$.
By the classification thm, there are 2 abelian groups of order 12:

$$\mathbb{Z}_2 \times \mathbb{Z}_6 \quad \text{and} \quad \mathbb{Z}_{12}$$

Consider the coset $(1,0)+N$. As an element of $\mathbb{Z}_4\times\mathbb{Z}_6/N$, its order is given by 4.

This shows that $\mathbb{Z}_4\times\mathbb{Z}_6/N \cong \mathbb{Z}_{12}$, since $\mathbb{Z}_2\times\mathbb{Z}_6$ has no order 4 elements. (Why?)

In fact, $(1,1)+N$ is a generator.

The Center and Commutator subgroups : 2 ways to measure how "abelian" a group is

Def The center of a group G is defined as

$$Z(G) = \{ g \in G \mid gx = xg \ \forall x \in G \}$$

Prop $Z(G) \triangleleft G$

Pf: Let $g_1, g_2 \in Z(G)$. Then ① $g_1 x = x g_1$ and ② $g_2 x = x g_2$ $\forall x \in G$.

② $\Rightarrow g_2^{-1} x = x g_2^{-1}$ $\forall x \in G$. Hence $(g_1 g_2^{-1})x = g_1(x g_2^{-1}) = x(g_1 g_2^{-1})$ $\forall x \in G$.

So $Z(G) < G$.

Let $g \in Z(G)$, $a \in G$. Then $gx = xg$ $\forall x \in G$

$\Rightarrow aga^{-1} = aa^{-1}g = g$. Hence $aZ(G)a^{-1} = Z(G)$ $\forall a \in G$.

So $Z(G) \triangleleft G$. #

Rmk: G is abelian iff $Z(G) = G$.

$G/Z(G)$ cyclic $\Rightarrow$ G abelian

Hence, if G is nonabelian and $|G| = pq$ $\Rightarrow$ $Z(G) = \{e\}$

e.g. • For S_3, the center is $Z(S_3) = \{id\}$.

• For $GL_n(\mathbb{R})$, $Z(GL_n(\mathbb{R})) = \mathbb{R} \cdot I_n$.

Def The subgroup $[G,G] < G$ generated by $\{aba^{-1}b^{-1} \mid a, b \in G\}$ is called the commutator subgroup of G (also denoted by G' or $G^{(1)}$)

(like 1st derivative of G)

Prop (1) $[G,G] \triangleleft G$

(2) For a normal subgroup $N \triangleleft G$,

$$G/N \text{ is abelian iff } N > [G,G].$$

Pf: (1) Let $S \subset G$ be any nonempty subset, and $H_S < G$ be the subgroup generated by S.

<u>Claim</u>: If $gSg^{-1} \subset S$ $\forall g \in G$, then $H_S \triangleleft G$.

Pf of claim: Recall that

$$H_S = \{ a_1^{n_1} \cdots a_k^{n_k} \mid a_1, \dots, a_k \in S, n_1, \dots, n_k \in \mathbb{Z} \}$$

If $gSg^{-1} \subset S$, then

$$g(a_1^{n_1} \cdots a_k^{n_k})g^{-1} = (ga_1g^{-1})^{n_1} \cdots (ga_kg^{-1})^{n_k} \in H_S$$

So $gH_Sg^{-1} \subset H_S$ and hence $H_S \triangleleft G$. #

Go back to $[G,G]$. Let $g \in G$. Then

$$g(aba^{-1}b^{-1})g^{-1} = (gag^{-1})(gbg^{-1})(gag^{-1})^{-1}(gbg^{-1})^{-1}$$

Hence $[G,G] \triangleleft G$.

(2) G/N is abelian $\Leftrightarrow$ $(Na)(Nb)=(Nb)(Na) \quad \forall a,b\in G$

$\Leftrightarrow \quad ab\in Nba \quad \forall a,b\in G$

$\Leftrightarrow \quad aba^{-1}b^{-1}\in N \quad \forall a,b\in G$

$\Leftrightarrow \quad [G,G]<N$ #

Rmk The quotient group $G/[G,G]$ is called the abelianization of G.

e.g. • For S_3, the commutator subgroup is $[S_3,S_3]=A_3$.

Pf: $\rho_1=\rho_2\mu_1\rho_2^{-1}\mu_1^{-1}$, $\rho_2=\rho_1\mu_1\rho_1^{-1}\mu_1^{-1}\in$ $\Longrightarrow$ $A_3<[S_3,S_3]$.

Here, $\rho_1=\rho=(1,2,3)$, $\rho_2=\rho_1^2$, $\mu_1=(1,2)$

Also, S_3/A_3 is abelian $\Longrightarrow$ $A_3>[S_3,S_3]$. #

• For $GL_n(\mathbb{R})$, $[GL_n(\mathbb{R}),GL_n(\mathbb{R})]=SL_n(\mathbb{R})$. (why?)