Direct Products

2013 03 15

saw on A2 this is a group →

Def Let $(G_1,*),(G_2,\diamond)$ be groups. Their direct product is the group $(G_1\times G_2,\cdot)$ where $G_1\times G_2=\{(g_1,g_2);\ g_i\in G_i\}$ and $(a_1,a_2)\cdot(b_1,b_2)=(a_1*b_1,\ a_2\diamond b_2)$.

We will abuse lots of notation.

Remark: We can similarly define $G_1\times\cdots\times G_n$. If $G_i=G_j=G\ \forall i,j$ then write G^n.

ex. $\mathbb{Z}_2^{\,2}=\{(0,0),(1,0),(0,1),(1,1)\}$ <draw table>

* has 5 subgroups

Many calculations in direct products reduce to calculations in the factors.

Lemma: Let $G=G_1\times\cdots\times G_n$, $n\geq 2$ (?) Then:

(1) $|G|=|G_1|\cdots|G_n|$

(2) $Z(G)=Z(G_1)\times\cdots\times Z(G_n)$

(3) If $H_1\leq G_1,\ldots,H_n\leq G_n$ then $H=H_1\times\cdots\times H_n\leq G$ and $H\trianglelefteq G\iff H_i\trianglelefteq G_i\ \forall i$.

(4) For $a=(a_1,\ldots,a_n)\in G$, $|a|=\operatorname{lcm}(|a_1|,\ldots,|a_n|)$

(5) G is abelian $\iff G_i$ is abelian $\forall i$.

Proof: (1),(3),(5) as exercise

(2): Let $x\in Z(G)$. Write $x=(x_1,\ldots,x_n)$. Will show $x_i\in Z(G_i)\ \forall i$.
Let $a\in G_i$. Define $g=(e_1,\ldots,\underbrace{a}_{i^{th}\text{ spot}},\ldots,e_n)\in G$. As $x\in Z(G)$ get

$xg=gx\Rightarrow(x_1,\ldots,x_ia,\ldots,x_n)=(x_1,\ldots,ax_i,\ldots,x_n)$

So $x_ia=ax_i\Rightarrow x_i\in Z(G_i)$. Thus $Z(G)\subseteq Z(G_1)\times\cdots\times Z(G_n)$
Other inclusion similar.

(4): Assume G is finite. $a^k=(a_1^k,\ldots,a_n^k)$. So $a^k=e$ iff $a_i^k=e_i\ \forall i$
iff $|a_i|\mid k\ \forall i$ ∎

Warning: Not all subgroups of G are products of subgroups of G_i's.

Direct products will be useful in understanding groups up to isomorphism.

ex $K=\{1,(12)(34),(13)(24),(14)(23)\}$
$K\cong(\mathbb{Z}_2)^2$ ← can think of it as a vec. sp.

Def Let G be a group. We say G is directly decomposable if there exists groups G_1, G_2 with $|G_1|, |G_2| > 1$ st $G \cong G_1 \times G_2$.
Otherwise, we say G is indecomposable.

Remark: Can easily show any finite group is isomorphic to a product of directly indecomposable groups.
~~Show~~ Should) Think of indecomposable groups as primes.
(Thm: uniqueness of factorization beyond course)

Theorem: Let G be a group. If $\exists H, K \lhd G$ st ~~$HK = \{e\}$~~, $HK = G$, $H \cap K = \{e\}$,
then $G \cong H \times K$, ie G is directly decomposable.
Proof: Recall from A5 that $kh = hk$ $\forall k \in K, h \in H$.
Define $\varphi: H \times K \to G$ by $\varphi((h,k)) = hk$
This is surjective as $HK = G$.
This is a homomorphism: $\varphi((h_1,k_1)(h_2,k_2)) = h_1 h_2 k_1 k_2 = h_1 k_1 h_2 k_2 = \varphi((h_1,k_1))\varphi((h_2,k_2))$ ✓
This is injective. Suppose $\varphi((h,k)) = e$. Then $hk = e \Rightarrow h^{-1} = k \in H \cap K = \{e\} \Rightarrow (h,k) = (e,e)$. ∎

2013 03 18

Def Let $H, K \leq G$. We say G is the *internal direct product* of H and K if (1) $H, K \trianglelefteq G$
(2) $H \cap K = \{e\}$
(3) $HK = G$

(*) Restatement of thm: If G is the i.d.p. of $H, K \leq G$ then $G \cong H \times K$.

When G is the i.d.p. of H, K, the $\cong$ is
$H \times K \to G = HK$ $\qquad$ $H \times \{1\} \to H$
$(h,k) \mapsto hk$ $\qquad$ $\{1\} \times K \to K$
$(h,1) \mapsto h$
$(1,k) \mapsto k$

ex. If $p \neq q$, $p \nmid n$, $q \nmid n$ primes, then $\mathbb{Z}_n$ directly decomp.
Equivalently, $m, n > 1$, $\gcd(m,n) = 1 \Rightarrow \mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$
Pf: Let $a = (1,1)$. So $|a| = \operatorname{lcm}(|1|, |1|) = \operatorname{lcm}(n,m) = nm$
Two cyclic groups of same size are $\cong$

(*) Theorem: Suppose $G \cong G_1 \times G_2$. Then $\exists H, K \leq G$ s.t. G is the i.d.p of H, K and $H \cong G_1$, $K \cong G_2$.
Proof: First assume $G = G_1 \times G_2$. Then clearly $H = G_1 \times \{e\} \cong G_1$, $K = \{e\} \times G_2 \cong G_2$.
Remain to show i.d.p: easy
In general, let $\varphi: G_1 \times G_2 \to G$, get $\bar{H}, \bar{K}$ by above, consider $K = \varphi(\bar{K})$, $H = \varphi(\bar{H})$ ∎

Cor: G is directly decomposable iff $\exists H, K \leq G$ s.t. G is the i.d.p. of H, K, and $\{e\} < H, K < G$
Proof: By (*), $G \cong H \times K$ with $|H|, |K| > 1$.
($\Rightarrow$): So $G \cong G_1 \times G_2$, $|G_1|, |G_2| > 1$. By (*), have $H \cong G_1, K \cong G_2$ non-triv.
Finally, if $H = G$ then $1 = H \cap K = G \cap K = K \neq \{1\}$. ∎

ex Every simple group is directly indecomposable.
Pf: Has no non-triv proper normal subgroups, so by Cor one does. ∎

ex $\mathbb{Z}_4$ is abelian, so all are normal. Not enough normal subgroups! (Need $H \cap K = \{e\}$)
Subgroups: $\langle 0 \rangle$, $\mathbb{Z}_4$, $\langle 3 \rangle$, ~~If were dir. decomp. would have $\mathbb{Z}_4 \cong \langle 3 \rangle \times \mathbb{Z}_4$~~
In general, $\mathbb{Z}_{p^2}$ is dir. indecom.

ex $\mathbb{Z}_{p^n}$ directly indecomp $\forall p$ prime, $n \geq 1$. Exercise: subgroups are $\langle p^i \rangle$, $0 \leq i \leq n$
Note any 2 subgroups $\neq \langle 0 \rangle$ contain $\langle p^{n-1} \rangle$ so can't have non-triv int

$\mathbb{Z}_p = \langle 1 \rangle \supset \langle p \rangle \supset \cdots \supset \langle p^{n-1} \rangle \supset \langle p^n \rangle = \langle 0 \rangle$

Scrap $r(p-1) = pr - r \leq pq$

$p(r-q) \leq r$

Have we turn our attention to abelian

2013 03 20

Prop: G finite, abelian. Then G is $\cong$ to dir. prod. of its Sylow subgroups.

(Sylow subgroups unique as abelian)

Pf: Idea: If $|G| = p^m q^n$ (p, q prime)

Then P, Q be the sylow p,q subgroups:

So $\gcd(|P|, |Q|) = 1 \Rightarrow P \cap Q = \{e\}$,

So $|PQ| = |P||Q| / |P \cap Q| = |G| \Rightarrow PQ = G$.

And $P, Q \trianglelefteq G$, so G is internal d.p. of $P, Q \Rightarrow G \cong P \times Q$

In general, $|G| = p_1^{m_1} \cdots p_t^{m_t}$

Let P_i be the Sylow p_i-subgroup. ↪ as G abelian

Let $k = p_1^{m_1} \cdots p_t^{m_t}$ Note $H = \{x \in G : x^k = 1\} \leq G$

Claim: $|H| | k$.

(Fill in)

(have $G \cong P_1 \times \cdots \times P_t$)

2013 03 22

Remark: Prev classes reduces the factorization problem (for finite/abelian) to # p-groups

Lemma: Let G be a finite abelian p-group that is not cyclic.
Let $a \in G$ be of maximum order. Then $\exists b \in G \setminus \langle a \rangle$ st $|b| = p$
Proof: Let $|G| = p^n$, $|a| = p^r$, $1 \leq r \leq n$ as not cyclic.
Let $b \in G \setminus \langle a \rangle$ of minimum order, So $|b| = p^s$ $1 \leq s \leq r$. Must show $s = 1$.
Note $|b^p| = p^{s-1} < |b|$.
By minimality, $b^p \notin G \setminus \langle a \rangle \Rightarrow b^p \in \langle a \rangle \Rightarrow b^p = a^m$ for some $m \in \mathbb{Z}^+$
Also $b^{p^r} = 1$ as $b^{p^s} = 1$ and $p^s \mid p^r$ as $s \leq r$.
So $1 = b^{p^r} = (b^p)^{p^{r-1}} = (a^m)^{p^{r-1}}$
So $|a^m| \leq p^{r-1} < |a|$ $\Rightarrow \gcd(m, p^r) \neq 1$ (otherwise $|a^m| = |a|$)
Thus $p \mid m$. Write $m = pt$. So $b^p = a^{pt}$. Let $x = a^{-t}b$.
Note: $x^p = a^{-pt} b^p = 1$ and $x \notin \langle a \rangle$ since else $b \in \langle a \rangle$.

So $x \neq e \Rightarrow |x| = p$. But $|b| \leq |x|$ by min. so $|b| = p$

Proposition: Let G be a finite abelian p-group. Let $a \in G$ be of maximum order. Then $\exists H \leq G$ st G is the i.d.p of $\langle a \rangle$ and H.
Proof: Let $|b| = p^n$. Induction on n.
Base case: G cyclic $\Rightarrow G = \langle a \rangle$, take $H = \{e\}$. (Check i.d.p properties)
Inductive case: If G is cyclic same as ↑, so assume G not cyclic.
By lemma, $\exists b \in G \setminus \langle a \rangle$, $|b| = p$. Let $\overline{G} = G/\langle b \rangle$.
Note $|\overline{G}| = p^{n-1}$ and is abelian.
Let $x \in G$. Then $|\overline{x}| \leq |x|$, where $\overline{x} = x\langle b \rangle$
Claim: $|\overline{a}| = |a|$ Note $\overline{a}^m = \overline{1} \Leftrightarrow a^m \in \langle b \rangle \Leftrightarrow a^m \in \langle a \rangle \cap \langle b \rangle \Rightarrow a^m \in \{e\}$
By ind, as $\overline{a}$ has max order, so $\exists \overline{H} \leq \overline{G}$.

... so $\exists \bar{H} \leq \bar{G}$ st $\bar{G}$ is i.d.p. of $\langle \bar{a} \rangle$, $\bar{H}$.
Let $H = \{x \in G : xB \in B\bar{H}\}$
Claim: $B \leq H$: Well $x \in B \Rightarrow xB = B = \bar{1} \in \bar{H} \Rightarrow x \in H$.
Remains to show G is i.d.p. of $\langle a \rangle$ and H.
- $\langle a \rangle H = G$: $g \in G \Rightarrow \bar{g} \in \bar{G} \Rightarrow \bar{g} = \bar{a}^m \cdot \bar{h} \Rightarrow g \in a^m h B, \Rightarrow g = \underbrace{a^m}_{\in \langle a \rangle} \underbrace{h b^\ell}_{\in H}$
- $\langle a \rangle \cap H = \{e\}$: $x \in \langle a \rangle \cap H \Rightarrow \bar{x} \in \langle \bar{a} \rangle \cap \bar{H} \Rightarrow$ (finish)

∎

Corollary: Every finite abelian p-group is $\cong$ to a direct product of cyclic groups.
Pf: G abelian, $|G| = p^n$. Induction on n.
If G is cyclic (eg $n=1$) then done.
Else pick $a \in G$ of max order. Prop above gives $H \leq G$ st G is the i.d.p. of $\langle a \rangle$ and H.
We know H abelian, $|H| = |G| / |\langle a \rangle| < |G|$.
By ind. hyp, H is $\cong$ to dir. prod. But $G = \langle a \rangle \times H \Rightarrow$ ✓ ∎

Cor (Fundamental Theorem of Finite Abelian Groups):
Every finite abelian group is $\cong$ to a dir. prod. of cyclic groups.
Moreover, each cyclic factor can be chosen to have prime ~~power~~ order.

Rmk: $|G| = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$.
so $\exists$ partition of α_i: $\alpha_i = \beta_1 + \cdots + \beta_{k_i}$, $\beta_1 \geq \cdots \geq \beta_{k_i} \geq 1$
$$P_i \cong \mathbb{Z}_{p_i^{\beta_1}} \times \cdots \times \mathbb{Z}_{p_i^{\beta_{k_i}}}$$

$$S_p \cong \left(\mathbb{Z}_{p_1^{\beta_1}} \times \cdots \times \mathbb{Z}_{p_1^{\beta_{k_1}}}\right) \times \cdots \times \left(\mathbb{Z}_{p_k^{\omega_1}} \times \cdots \times \mathbb{Z}_{p_k^{\omega_{k_k}}}\right)$$

$p_1^{\beta_1}, \ldots, p_1^{\beta_{k_1}}, \ldots, p_k^{\omega_1}, \ldots, p_k^{\omega_{k_k}}$ are the <u>elementary divisors</u> of G. They are unique.

How many abelian groups of order 72? (up to $\cong$)
Note $72 = 2^3 \cdot 3^2$. #Partitions of 3 = 3, #partitions of 2 = 2
$$\Rightarrow \left\{ \begin{matrix} \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \\ \mathbb{Z}_4 \times \mathbb{Z}_2 \\ \mathbb{Z}_8 \end{matrix} \right\} \times \left\{ \begin{matrix} \mathbb{Z}_3 \times \mathbb{Z}_3 \\ \mathbb{Z}_9 \end{matrix} \right\} \rightarrow 6$$

2013 03 27

Let G be a finite abelian group, $|G| = 2^7 3^3 5^3$
Say it's elementary divisors are $4,4,4,4,2,27,9,3,3,5,5,5$.
Then $G \cong (\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_2) \times (\mathbb{Z}_{27} \times \dots) \times (\mathbb{Z}_5 \times \dots)$

$\Rightarrow G \cong (\mathbb{Z}_4 \times \mathbb{Z}_{27} \times \mathbb{Z}_5)$
$\times (\mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5)$
$\times (\mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5)$
$\times (\mathbb{Z}_2 \times \mathbb{Z}_3)$
$\times (\mathbb{Z}_3)$

but $\gcd(4,27,5) = 1$, so we get
$\mathbb{Z}_{540} \times \mathbb{Z}_{180} \times \mathbb{Z}_{180} \times \mathbb{Z}_6 \times \mathbb{Z}_3$

This is called the invariant factor factorization
The invariant factors (here) are $540, 180, 180, 6, 3$

Note $3 \mid 6 \mid 180 \mid 180 \mid 540$
More generally:

Fundamental Thm of Finite Abelian groups, invariant factor version:
If G is a finite group, then $\exists n_1, \dots, n_r \in \mathbb{Z}^{\geq 2}$ s.t. $n_r \mid n_{r-1}, \dots, n_2 \mid n_1$
with $G \cong \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_r}$.
Moreover, these are unique.

Lemma: Suppose G is a finite abelian group, G not cyclic. Then $\exists n > 1$ s.t. $|\{x \in G : x^n = e\}| > n$
Write $G = \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_r}$ with $n_r \mid n_{r-1}, \dots$
As not cyclic, $r \geq 2$.
Note $n_r \mid n_i \ \forall i$, so $\mathbb{Z}_{n_i}$ has subgroup H_i of size n_r.
Then $H_1 \times \dots \times H_r \leq \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_r}$
in
$\{x \in \mathbb{Z}_{n_1} \times \dots ; nx = 0\}$

Gives n^r elements in $\mathbb{Z}_{n_1} \times \dots$ of order divides n
Since $G \cong \mathbb{Z}_{n_1} \times \dots$, G also has n^r elmts whose order divides n

Cor: If $\mathbb{F}$ is a finite field, then $(\mathbb{F}^\times, \cdot)$ is a cyclic group
Pf: If it's not cyclic, then $\exists n > 1$ s.t. $|\{x \in \mathbb{F} : x^n = 1\}| > n \Rightarrow x^n - 1$ has more than n roots. $**$