Some Group Theory Class Notes

Class February 23

1. Direct Products and Finite Abelian Groups

Definition 0.1. G always denotes a group. G is the inner direct product of the subgroups $A, B \leq G$ if i) $A \lhd G$, $B \lhd G$ ii) $A \cap B = \{e\}$ iii) $G = AB$. The notation for direct products is $G = A \times B$.

Lemma 0.2. *Assume $G = A \times B$.*
(a) A and B commute element-wise i.e. $ab = ba\ \forall a \in A, b \in B$.
(b) if A and B are abelian, then so is G.

Proof. (a) Consider the commutators $[a, b] := (aba^{-1})b^{-1} = a(ba^{-1}b^{-1}) \in A \cap B = \{e\}$
$\implies aba^{-1}b^{-1} = e \implies ab = ba\ \forall a \in A, b \in B$
(b) $g_1, g_2 \in G \implies \exists a_1, a_2 \in A, b_1, b_2 \in B$ s.t. $g_1 = a_1b_1$ and $g_2 = a_2b_2 \implies g_1g_2 = a_1b_1a_2b_2 = a_1a_2b_1b_2$ and because A, B are abelian, this equals $a_2(a_1b_2)b_1 = a_2b_2a_1b_1 = g_2g_1$ $\square$

Example 0.3. (a) $V =< (12)(34) > \times < (13)(24) >\cong \mathbb{Z}_2 \times \mathbb{Z}_2$
(b) $U(8) = \{[1], [3], [5], [7]\} =< [3] > \times < [5] >\cong \mathbb{Z}_2 \times \mathbb{Z}_2$.
(c) $\mathbb{Z}_6 =< [3] >\cong \mathbb{Z}_3\times < [2] >\cong \mathbb{Z}_2$
(d) $D_6 = \{b^i, ab^i \mid 0 \leq i \leq 5\}$ such that $a^2 = b^6 = e$, $aba^{-1} = aba = b^{-1}$. Therefore, $D_6 \cong< b^3 > \times\{e, b^2, b^4, a, ab^2, ab^4\} \implies D_6 \cong \mathbb{Z}_2 \times D_3$
(e) By contrast, neither D_4 nor Q_8 can be written as direct products of two proper subgroups (Exercise).
(f) Trivially, $\forall G, G = G \times \{e\}$

Lemma 0.4. *If $|G|= p^2$, p is prime, then either G is cyclic or $G = A \times B(\cong \mathbb{Z}_p \times \mathbb{Z}_p)$ with subgroups A and B of order p.*

Proof. G is a p-group so the center $Z(G)$ is nontrivial. Assume $Z(G) = p \implies G/Z(G) \cong \mathbb{Z}_p$ $\implies G/Z(G)$ is cyclic and therefore G is abelian. But this is a contradiction, because if G is abelian, $|G|= |Z(G)|$ by definition.Therefore, we know that G is abelian and $G = Z(G)$.
Assume G is not cyclic $\implies |g|= p\ \forall g \in G \setminus \{e\}$. Pick any $a \in G \setminus \{e\}$ and set $A =< a >\leq G$ $\implies |a|= |A|= p$. Therefore, $|G \setminus A|= p^2 - p > 0 \implies G \setminus A \neq \emptyset$. Pick $b \in G \setminus A$ and set $B :=< b >\leq G \implies |b|= |B|= p$.
Now, check (1) $A \lhd G, B \lhd G$ because G is abelian. (2) $A \cap B = \{e\}$. If $e \neq x \in A \cap B$ $\implies |x|= p \implies A =< x >= B \implies b \in A$ which is a contradiction. (3) $G = AB$. $AB = \frac{|A||B|}{|A\cap B|} = \frac{p*p}{1} = p^2 = |G| \implies G = AB$ $\square$

Class February 26

Remark 0.5. If $a, b \in G$ with $|a|, |b|< \infty$, then $|ab||\ lcm(|a|, |b|)$ of $ab = ba$. If $ab \neq ba$, you cannot say anything about $|ab|$. If $ab = ba$, then $|ab|< lcm(|a|, |b|)$ is possible in general (e.g. $b = a^{-1}$). If $ab = ba$ and $gcd(|a|, |b|) = 1$, then $|ab|= |a||b|= lcm(|a|, |b|)$. This uses the fact that $< a > \cap < b >= \{e\}$.

Definition 0.6. The (outer) direct product of the groups A, B is defined as $A \times B = \{(a, b)|a \in A, b \in B\}$ as set with a binary operation $\implies (a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2)\ \forall a_1, a_2 \in A$ and $\forall b_1, b_2 \in B$.

This yields a group since (i) $A \times B$ satisfies associativity since A and B do (ii) $e_{A\times B} = (e_A, e_B)$ and (iii) $(a,b)^{-1} = (a^{-1}, b^{-1})$ for $a \in A, b \in B$.
Define $\iota_A : A \to A \times B$ which maps $a \to (a,e)$ and $\iota_B : B \to A \times B$ which maps $b \to (e,b)$. Then, ι_A, ι_B are injective group homomorphisms.
$A \cong \iota_A(A) =: A' = \{(a,e) | a \in A\} \leq A \times B$ and $B \cong \iota_B(B) =: B' = \{(e,b) | b \in B\} leq A \times B$.

Remark 0.7. Properties of subgroups A', B' of $A \times B$:
(1) $A', B' \lhd A \times B$, e.g. $(\tilde{a}, b)(a,e)(\tilde{a}^{-1}, b^{-1}) = (\tilde{a}a\tilde{a}^{-1}, beb^{-1}) = (\tilde{a}a\tilde{a}^{-1}, e) \in A'$
(2) $A' \cap B' = \{(a,b) \in A \times B | b = e, a = e\} = \{(e,e)\}$.
(3) $G = A'B' \implies$ given $(a,b) \in A \times B$, then $(a,b) = (a,e)(e,b)$
The consequence is that the outer product equals the inner product such that $A \times B = A' \times B'$

Lemma 0.8. *Assume that $G = A \times B$ (inner; $A, B \leq G$) and that A', B' are groups with $A' \cong A$ and $B' \cong B$. Then, $G \cong A' \times B'$ (outer).*

An application of this is that if $|G| = A \times B$ with $|A| = |B| = p \implies G \cong \mathbb{Z}_p \times \mathbb{Z}_p$ (outer).

Class February 28

Lemma 0.9. *If $G = A \times B$ with subgroups $A, B \leq G$ and $a \in A, b \in B$ then $|ab| = lcm(|a|, |b|)$ ($= \infty$ if $|a| = \infty$ or $|b| = \infty$).*

Proof. A previous lemma revealed that if $G = A \times B$, then A and B commute element-wise i.e. $ab = ba$ $\forall a \in A, b \in B$. This implies that $(ab)^n = ab * ... * ab = a^n b^n$ $\forall n \in \mathbb{N} \implies (ab)^n = e \Leftrightarrow a^n b^n = e \Leftrightarrow a^n = b^{-n} \in A \cap B = \{e\}$. $\therefore (ab)^n = e \Leftrightarrow a^n = e$ and $b^n = e \implies$ if $|a| = \infty$ or $|b| = \infty$, then $a^n \neq e$ $\forall n \in N$ or $b^n \neq e$ $\forall n \in N$. Now, assume $k = |a| < \infty$ and $l = |b| < \infty$. $ab)^n = e \Leftrightarrow a^n = e$ and $b^n = e$ $\Leftrightarrow k \mid n$ and $l \mid n \Leftrightarrow lcm(k,l)$. Hence, $|ab| = min\{n \in \mathbb{N} \mid (ab)^n = e\} = lcm(k,l) = lcm(|a|, |b|)$ ☐

Remark 0.10. This is also true for the outer direct product $A \times B$, i.e. for $a \in A$ and $b \in B$, we get $|(a,e) * (e,b)| = |(a,b)| = lcm(|a|, |b|)$. This follows from the previous lemma and $A \times B = A' \times B'$ (outer direct product equals inner direct product). More remarks follow:

1. $a_1, b_1) * (a_2, b_2) = (a_1a_2, b_1b_2)$

   Example 0.11. $\mathbb{Z}_4 \times \mathbb{Q}_8 \rightsquigarrow ([k], x)([l], y) = ([k+l], xy)$ Moreover, note that all subgroups of $\mathbb{Z}_4$ and all subgroups of $\mathbb{Q}_8$ are normal but $\mathbb{Z}_4 \times \mathbb{Q}_8$ has a non-normal subgroup.

2. $H \leq A, K \leq B \implies H \times K = \{(h,k) \mid h \in H, k \in K\} \leq A \times B$. But not all subgroups of $A \times B$ need to be of this form.

3. $H \times K \lhd A \times B \Leftrightarrow H \lhd A$ and $K \lhd B$ (check both directions with definitions).

Lemma 0.12. *$A, B \leq G$, $G = A \times B$ and $A' \cong A, B' \cong B$. Then, $G \cong A' \times B'$ (outer direct product)*

Proof. $A' \cong A$ means $\exists$ isomorphism $\varphi_A : A' \to A$, $B' \cong B$ means $\exists$ isomorphism $\varphi_B : B' \to B$. Therefore, define a map $\varphi : A' \times B' \to G$ which maps $(a', b') \to \varphi_A(a')\varphi_B(b')$
NTS that φ is in fact an isomorphism:
To show that φ is a group homomorphism: $\varphi((a_1', b_1')(a_2', b_2')) = \varphi((a_1'a_2', b_1'b_2')) = \varphi_A(a_1'b_2')\varphi_B(b_1'b_2') = \varphi_A(a_1')\varphi_A(a_2')\varphi_B(b_1')\varphi_B(b_2') = \varphi_A(a_1')\varphi_B(b_1')\varphi_A(a_2')\varphi_B(b_2') = \varphi((a_1', b_1')\varphi((a_2', b_2') \rightsquigarrow$ group homomorphism.

φ is injective since φ_A and φ_B are injective; check $\ker(\varphi) = \{(e,e)\}$ (also use $A \cap B = \{e\}$). $\varphi_A(a')\varphi_B(b') = e \in G \implies \varphi_A(a') = e$ and $\varphi_B(b') = e$.
φ is surjective since φ_A and φ_B are surjective. Given $g = ab \in G$ $(a \in A, b \in B)$, find preimages $a' \in A, b' \in B \implies \varphi((a',b')) = ab = g$.
$\therefore \varphi$ is an bijective homomorphism, or an isomorphism. $\square$

Proposition 0.13. *If $m,n \in \mathbb{N}$ with $gcd(m,n) = 1$, then $\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m$*

Proof. $\mathbb{Z}_{nm} = \{[k]_{nm} \mid 1 \leq k \leq nm\}$. Set $a := [m]_{nm}$, $A :=< a > \implies |a|= |A|= n$ and $b := [n]_{nm}$, $B :=< b > \implies |b|= |B|= m$. Claim: $\mathbb{Z}_{nm} = A \times B$ (inner direct product). To show this, (1) $A, B \lhd \mathbb{Z}_{nm}$ because $\mathbb{Z}_{nm}$ is abelian (2) $x \in A \cap B \implies |x|| \; gcd(|A|,|B|) = gcd(n,m) = 1 \implies x = [0]_{nm} = [nm]_{nm}$ (3) $|A + B|= \frac{|A|*|B|}{|A \cap B|} = \frac{n*m}{1} = nm = |\mathbb{Z}_{nm}| \implies A + B = \mathbb{Z}_{nm}$ ("Chinese Remainder Theorem"). $A \cong \mathbb{Z}_n$, $B \cong \mathbb{Z}_m \implies \mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$ $\square$

Discussion 0.14. Direct products with > 2 factors can be done in two ways:

1. inductively: $A_1 \times ... \times A_n = (A_n \times ... \times A_{n-1}) \times A_n$
2. "inner": subgroups $A_1, ..., A_n \leq G$ such that (1) $A_i \lhd G \; \forall i$ (2) $A_i \cap A_1...A_{i-1}A_{i+1}...A_n = \{e\}$ $(\implies A_i \cap A_j = \{e\})$
3. $G = A_1...A_n$

Example 0.15. $G = \mathbb{Z}_2 \times \mathbb{Z}_2$. $A_1 =< ([1],[0]) >$, $A_2 =< ([0],[1]) >$, $A_3 =< ([1],[1]) >$. $A_i \cap A_j = \{([0],[0])\} \; \forall i \neq j$, but $G \neq A_1 \times A_2 \times A_3$ (must have $|G|= \prod_{i=1}^{n} |A_i|$) if $G = A_1 \times ... \times A_n$. "outer": Given groups $A_1, ..., A_n \rightsquigarrow A_1 \times ... \times A_n = \{(a_i)_{1 \leq i \leq n} \mid a_i \in A \; \forall i\}$ with multiplication $(a_i)(a_{i'}) := (a_i a_{i'})_{1 \leq i \leq n}$

Remark 0.16. $G = A_1 \times ... \times A_n$ (inner), then $A_i \cap A_j = \{e\} \; \forall i \neq j \implies A_i$ and A_j commute element-wise (using $A_i, A_j \lhd G$). Then it follows that (outer) $A_1 \times ... \times A_n \cong G$ $(= A_1 \times ... \times A_n$ (inner))

Class March 2

Proposition 0.17. *Let G be a finite group with $|G|= \prod_{i=1}^{n} p_i^{e_i}$ such that $p_1, ..., p_n$ are distinct primes. Pick $P \in Syl_P(G) \; \forall i$. If $n_p = 1$ $(\Leftrightarrow P \lhd G)$ $\forall i$, then $G = P_1 \times ... \times P_n$. Note that the assumption that $P_i \lhd G$ $(\Leftrightarrow n_{p_i} = 1)$ applies in particular to finite abelian groups.*

Proof. Verify (1)-(3) of an inner direct product (1) $P_i \lhd G \; \forall i$ (Consequence: Any product of some of the P_i's is a (normal) subgroup of G. We apply $|AB|= \frac{|A|*|B|}{|A \cap B|} \; \forall A, B \leq G \rightsquigarrow |P_1...P_l|= \prod_{i=1}^{l} P_i^{n_i}$ $(l \leq k)$, $|P_1...P_{i-1}P_{i+1}...P_k|= \frac{|G|}{P_i^{n_i}} =: \hat{P}_i$ (2) $P_i \cap \hat{P}_i = \{e\}$ since $gcd(|P_i|, |\hat{P}_i|) = gcd(p_i^{n_i}, \frac{|G|}{P_i^{n_i}}) = 1$
(3) $|P_1...P_k|= \prod_{i=1}^{k} P_i^{n_i} |G| \implies P_1...P_k = G$ $\square$

Remark 0.18. G finite, p prime, $p \mid |G| \implies$ by the 2nd Sylow Theorem, any element of p-power order is contained in some Sylow p-subgroup of G. $x \in G$, $|x|= p^i \implies |< x >|= p^i \implies \exists P \in Syl_P(G) : x \in P$. If $n_p = 1$ i.e. $Syl_P(G) = \{P\}$, then $P = \{x \in G \mid |x|= p^i$ with $i \in \mathbb{N}_0\}$ $(|e|= p^0)$. ($\supseteq$ as remarked and $\subseteq$ because any element of the p-subgroup P must have p-power order)

Corollary 0.19. *Two finite abelian groups G and G' are isomorphic $\Leftrightarrow$ they have isomorphic Sylow subgroups*

Proof. ($\implies$) $\exists$ isomorphism $\varphi : G \to G'$. $G = P_1 \times ... \times P_k$ and $G' = P_1' \times ... \times P_k'$. $G \cong G' \implies$ the same primes $p_1, ..., p_k$ divide $|G|$ and $|G'|$. Note that since φ is an isomorphism, $|x|= |\varphi(x)|$ $\forall x \in G$. $\{x \in G \mid |x| \text{ is a power of } p_i\} = P_i \implies \varphi(P_i) = \varphi(\{x \in G \mid |x| \text{ is a power of } p_i\}) = \{x' \in G \mid |x'| \text{ is a power of } p_i\} = P_i'$. Consequence: By restriction, φ induces an isomorphism between P_i and P_i' for any $1 \leq i \leq k$.
($\Leftarrow$) $G = P_i \times ... \times P_k$, $G' = P_1' \times ... \times P_k'$. Assume $\exists$ isomorphisms $\varphi_i : P_i \to P_i'$ $\forall 1 \leq i \leq k$. Then, define $\varphi : G \to G'$ by $\varphi(x_1, ..., x_k) := \varphi_1(x_1)...\varphi_k(x_k)$ whenever $x_i \in P_i$ $\forall i$. Note the following (i) every $g \in G$ can be written in this way since $G = P_1...P_k$ (ii) if $x_1...x_k = y_1...y_k$ with $x_iy_i \in P_i$ $(1 \leq i \leq k)$ then $x_i = y_i$ $\forall i$ and also P_i and P_j commute $\forall i \neq j$ e.g. $y_1^{-1}x_1 = y_2x_2^{-1}...y_kx_k^{-1} \in P_1 \cap P_2 \cap ... \cap P_k = \{e\}$. Now check φ is a group isomorphism (exercise). □

Consequence: The analysis of finite abelian groups reduces to the analysis of finite abelian p-groups.

Proposition 0.20. *If G is a finite abelian p-group and $a \in G$ with $|a|= max\{|b| | \ b \in G\}$, then there exists a subgroup $H \leq G$ such that $G =< a > \times H$*

Proof. Algebra: Pure and Applied by Aigli (page 124/125) □

Corollary 0.21. *Induction on $|G|$, if G is abelian, $|G|= p^n$, p prime, then there exists $e_1, ..., e_r \in \mathbb{N}$ such that $e_1 \geq ... \geq e_r \geq 1$, $e_1 + ... + e_r = n$ and $G \cong \mathbb{Z}_pe_1 \times ... \times \mathbb{Z}_pe_r$*

Proposition 0.22. *G abelian, $|G|= p^n$, p prime. Assume $G = \mathbb{Z}_pe_1 \times ... \times \mathbb{Z}_pe_r$, $e_1 \geq ... \geq e_r \geq 1$, $\cong \mathbb{Z}_pe_1' \times ... \times \mathbb{Z}_pe_s'$, $e_1' \geq ... \geq e_s' \geq 1$. Then $r = s$ and $e_i = e_i'$ $\forall$ $1 \leq i \leq r$*

Proof. Proposition 3.4.13 on Page 127 □

Theorem 0.23. *Fundamental Theorem of Finite Abelian Groups. If G is a finite abelian group, $|G|= \prod_{i=1}^{k} p_i^{n_i}$ with distinct primes $p_1, ..., p_k$, then there exist uniquely determined $r_i \in \mathbb{N}$; $e_{ij} \in \mathbb{N}$ $1 \leq j \leq r_i$, $e_{i1} \geq ... \geq e_{ir_i}$ and $e_{i1} + ... + e_{ir_i} = n_i$ such that $G \cong \mathbb{Z}_{p_1}e_{11} \times ... \times \mathbb{Z}_{p_1}e_{1r_1} \times ... \times \mathbb{Z}_{p_k}e_{kr_i}$.*

Proof. Exercise that uses previously stated propositions and corollaries. □

Example 0.24. Determine, up to isomorphism, all abelian groups of order 72. $72 = 2^3 * 3^2$. Therefore, abelian groups of order 8: $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ | 3. Abelian groups of order 9: $\mathbb{Z}_9$, $\mathbb{Z}_3 \times \mathbb{Z}_3$ | 2. Abelian groups of order 72 $\implies$ there are $3 * 2 = 6$ (form all the combinations between abelian groups of order 8 and 9).

Class March 12

Remark 0.25.

1. G is called solvable if $\exists$ a chain $G = G_0 \rhd G_1 \rhd ... \rhd G_n = \{e\}$ s.t. $G_{i+1} \lhd G_i$ and G_i/G_{i+1} is abelian ($\Leftrightarrow [G_i, G_i] \subseteq G_{i+1}$). Important Fact: $N \lhd G$ such that N and G/N are solvable. Then also G is solvable. Using Sylow $\implies$ all groups of order ¡60 are solvable

2. G is called nilpotent if $\exists$ a chain $G = G_0 \rhd G_1 \rhd ... \rhd G_n = \{e\}$ such that $G_i \lhd G$ $\forall$ i and $G_i/G_{i+1} \leq Z(G/G_{i+1})$ ($\Leftrightarrow [G, G_i] \subseteq G_{i+1}$). Warning: $N \lhd G$; N, G/N are nilpotent $\not\Rightarrow$ G is nilpotent.

   Example 0.26. $G = S_3$, $N = A_3 \cong \mathbb{Z}_3$ abelian. $G/N = S_3/A_3 \cong \mathbb{Z}_2$ abelian. But S_3 is NOT nilpotent

   But, $G/Z(G)$ nilpotent $\implies$ G is nilpotent

(a) Every finite p-group is nilpotent (follows from the fact every p-group has a nontrivial center + induction).

(b) If G is finite, then G is nilpotent $\Leftrightarrow$ all Sylow subgroups of G are normal $\Leftrightarrow$ G is a direct product of its Sylow subgroups.