Math 332 Thursday, March 5

* Announce talk
* Midterm
* HW due Thursday

Today:
* quiz
* another Cayley thm.
* isomorphism thm.
  - short exact sequences.

Quiz

1. What is an internal product of groups?
2. State and prove the first isomorphism theorem for groups. You may use the fact that the kernel of a homomorphism is normal.

Thm. (Cayley) Let G be a finite group with order divisible by some prime p. Then G has an element of order p.

Pf/ We first consider the case where G is abelian. (This was a HW problem.) Take $x \neq e$ in G if $|x|$ is divisible by p, say $|x| = mp$, then x^m has order p, and we're done. Otherwise, $\langle x \rangle \trianglelefteq G$ since G is abelian, and $G/\langle x \rangle$ has order divisible by p and strictly smaller than G. By induction, $G/\langle x \rangle$ has an element $y\langle x \rangle$ of order p. Now,

$(y\langle x\rangle)^{|y|} = y^{|y|}\langle x\rangle = e\langle x\rangle = \langle x\rangle =$ identity in $G/\langle x\rangle \Rightarrow p \mid |y|$ ②

$\Rightarrow |y| = mp$ for some $m \Rightarrow y^m$ has order p.

Now suppose G is not abelian. Write G as a disjoint union of conjugacy classes: $G = \bigcup_{i=1}^{t} \mathrm{conj}(x_i)$, and consider the class equation:

$$|G| = |Z(G)| + \sum_{x_i : |\mathrm{conj}(x_i)|>1} \frac{|G|}{\underbrace{|C(x_i)|}_{|\mathrm{conj}(x_i)| = [G : C(x_i)]}}$$

$C(x_i) =$ centralizer of x_i
$= \{g \in G : gx_i = x_i g\}$

For those x_i such that $|\mathrm{conj}(x_i)| > 1$, we have $[G : C(x_i)] > 1$, so $C(x_i) \lneq G$. If any of these $C(x_i)$ has order divisible by p, we are done by induction. Otherwise, reducing the class equation mod p gives $0 = |Z(G)| \mod p$. So p divides the order of the group $Z(G) < G$. Since $Z(G)$ is abelian, it has an element of order p by the first part of this proof. $\square$

Thm. Let G be a group with subgroup $H < Z(G)$ such that G/H is cyclic. Then G is abelian.

Pf/ Text. $\square$

Thm. Let p be prime. Every group of order p^2 is abelian.

Pf/ Let G be a group of order p^2. We would like to show $Z(G) = G$. If not, then $G/Z(G)$ has order p, hence is cyclic. So by the previous theorem, G is abelian and $Z(G) = G$, a contradiction. $\square$

First Isomorphism Theorem

Def. If $N \trianglelefteq G$ define the **quotient mapping** $\pi : G \to G/N$.
$$g \mapsto gN$$
This is a homomorphism of groups

II. First Isomorphism Theorem Let $\varphi : G \to G'$ be a homomorphism of groups. Then there is a well-defined isomorphism

$$\begin{aligned} G/\ker\varphi &\xrightarrow{\tilde{\varphi}} \operatorname{im}\varphi \\ a\ker\varphi &\longmapsto \varphi(a) \end{aligned}$$

Universal property of the quotient mapping Every homomorphism $\varphi : G \to G'$ factors through the quotient mapping:

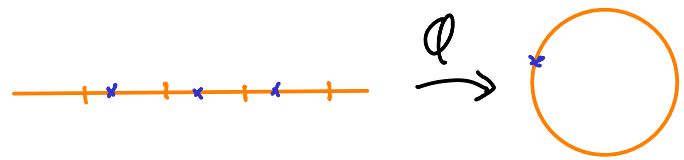
$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[dr, "\pi"'] & G' \\ & G/\ker\varphi \arrow[u, dotted, "\exists!\, \tilde{\varphi}"'] \end{tikzcd}$$

The word *factor* here applies since $\varphi = \tilde{\varphi} \circ \pi$. Note we have factored φ into a surjection followed by an injection.

Pf/ Let $\tilde{\varphi}(a\ker\varphi) := \varphi(a)$ and check the details. $\square$

Example $\varphi : \mathbb{R} \longrightarrow S^1 := \{ z \in \mathbb{C} : |z| = 1 \}$

$t \longmapsto e^{2\pi i t}$



The mapping φ is a surjective homomorphism with kernel $\mathbb{Z}$. So φ induces the isomorphism $\mathbb{R}/\mathbb{Z} \longrightarrow S^1$.

Exact Sequences The sequence of group homomorphisms

$$G'' \xrightarrow{\varphi} G \xrightarrow{\psi} G'$$

is **exact** at G if $\operatorname{im} \varphi = \ker \psi$.

Def. A **short exact sequence** (s.e.s.) of groups is a sequence of homomorphisms

$$1 \longrightarrow N \xrightarrow{\varphi} G \xrightarrow{\psi} H \longrightarrow 1$$

exact at N, G, and H. Here, denotes the group with just 1 element.

Remarks If $1 \hookrightarrow N \xrightarrow{\phi} G \xrightarrow{\psi} H \to 1$ is a s.e.s. of groups,

(1) ψ is surjective,

(2) ϕ is injective, thus, we may assume $N < G$.

(3) $N \lhd G$ and $H \cong G/N$.

Pf/ HW for Tuesday. $\square$

Example of a ses. Let H, K be groups. Then the following is a s.e.s.:

$$
\begin{array}{ccccccccc}
1 & \longrightarrow & H & \to & H \times K & \longrightarrow & K & \longrightarrow & 1 \\
 & & & & (h,k) & \longmapsto & k & & \\
 & & h & \longmapsto & (h,1) & & & &
\end{array}
$$

Characterization of normality: $N < G$ is normal iff

$N = \ker \varphi$ for some homomorphism $\varphi : G \to G'$.

Pf/ ($\Leftarrow$) Suppose $\varphi : G \to G'$ and $N = \ker \varphi$. Then $N \trianglelefteq G$ by HW.

($\Rightarrow$) Suppose $N \trianglelefteq G$. Then $N = \ker \left(G \xrightarrow{\pi} G/N \right)$. $\square$

III Internal products

We've already talked about products and coproducts (direct sums) of groups. Here are some related ideas.

Prop. If H, K are subgroups and $H \trianglelefteq G$, then HK is a subgroup of G.

Pf/ See text. $\square$ (What about KH?).

Prop. Let H, K be normal subgroups of G with $HK = G$ and $H \cap K = \{e\}$. Then $G \cong H \times K$. In this case we say G is an internal direct product of H and K.

Pf/ See text. $\square$

Example

* $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Let $H = \{(a,0) : a \in \mathbb{Z}/2\mathbb{Z}\} \leq G$

$K = \{(0,a) : a \in \mathbb{Z}/2\mathbb{Z}\} \leq G$.

Then $H, K \trianglelefteq G$ since G is abelian, $G = H + K$, and $H \cap K = \{(0,0)\}$.