Reminder - please pick up graded assignments from CA mailboxes

Homework - prepare for the midterm! Know: · vocab

· main theorems

· examples and applications

Review

1. Motions in $\mathbb{R}^n$

$$m = \underset{\substack{\text{poss. trivial} \\ \cap \\ \mathbb{R}^n}}{(\text{translation})} \underbrace{\underset{\substack{\text{poss. trivial} \\ \cap \\ SO(n)}}{(\text{rotation})} \underset{\substack{\text{or identity} \\ \cap \\ \langle \pm 1 \rangle \cong \langle r \rangle}}{(\text{reflection})}}_{\in O(n) \cong SO(n) \times \langle r \rangle}$$

the set of translations $T (\cong \mathbb{R}^n) \triangleleft \{\text{Motions}\}$

· arises as kernel of the map $\{\text{Motions}\} \longrightarrow \mathbb{R}^n$

2. Motions in the plane

Classification of <u>discrete</u> subgroups

· analysis via decomposition into a translation subgroup (lattice) and a subgroup of $O(2)$ (point group)

· subgroups of $O(2)$ that arise are C_n, D_{2n} where $n = 1, 2, 3, 4,$ or 6

- it is useful to generalize these ideas to ...

3. Abstract symmetry and group actions

a <u>group action</u> $G \circlearrowright S$ has the properties $1 \cdot s = s$, $gg' \cdot s = g \cdot (g' s)$ $\forall s \in S$, $g, g' \in G$

given $s \in S$, the <u>orbit</u> $O_s = \{g \cdot s \mid g \in G\}$ and

the <u>stabilizer</u> $G_s = \{g \in G \mid g \cdot s = s\}$

<u>prop</u>: $G/G_s \xrightarrow{\sim} O_s$ as a G-set (a set equipped with a group action)

$gG_s \longmapsto g \cdot s$

assuming G is finite, we have $|G| = |G_s| \cdot |O_s|$

prop: $G_{g \cdot s} = g G_s g^{-1}$

examples of applications of these formulas

fix a group G and a set S

<u>prop</u>: there is a 1-1 correspondence between actions of G on S and group homomorphisms $G \to \mathrm{Sym}(S)$

$$\left\{ \begin{matrix} \text{actions} \\ G \circlearrowright S \end{matrix} \right\} \longleftrightarrow \left\{ \begin{matrix} \text{gp. hom.} \\ G \to \mathrm{Sym}(S) \end{matrix} \right\}$$

$$G \circlearrowright S \longmapsto [g \mapsto [s \mapsto g \cdot s]]$$

$$g \cdot s = \varphi(g) \cdot s \longleftarrow [\varphi : G \to \mathrm{Sym}(S)]$$

3. Abstract symmetry and group actions (continued)

So: if $|S| = n$, $\mathrm{Sym}(S) \cong S_n$, and $G \circlearrowright S$ gives a homomorphism $G \to S_n$

In particular, $G \circlearrowright S = G$ by left translation, so if $|G| = n$, we have a group homomorphism

$$\varphi : G \hookrightarrow S_n$$

that is injective ($\varphi(g)$ is determined by $g \cdot e = g$).

· Another action of $G \circlearrowright G$ is given by conjugation $g \cdot x = gxg^{-1}$

$$|G| = \sum_{\substack{O \text{ orbit} \\ \text{in } G \text{ for} \\ \text{this action}}} |O| = \sum_{\substack{\text{conj.} \\ \text{classes} \\ C}} |C| \qquad \underline{\text{class equation}}$$

$C = \{x\}$ is a conjugacy class $\Leftrightarrow x \in Z$ = center of G

applications to p-groups

· has center of order > 1

· every group of order p^2 is abelian

<u>def</u>: a <u>simple</u> group G has the property that $H \trianglelefteq G \Leftrightarrow H = 1, G$

· these groups are structurally important, for if G is simple and $f : G \to G'$ is a group homomorphism, then f is either injective or trivial.

· If $H \trianglelefteq G$, $H = \bigcup\{\text{conjugacy classes}\}$

∴ the class equation plus the fact that $|H| \mid |G|$ can sometimes be used to show that a group is simple.

4. Sylow theory

let G be a group of order $p^e m$ ($e \geq 1$, $p \nmid m$). Then

· $n_p(G)$ = # of Sylow p-subgroups (subgroups of order p^e) satisfies $n_p(G) \equiv 1 \pmod p$, $n_p(G) \mid m$

· every two Sylow p-subgroups are conjugate

· if $K \subset G$ is any subgroup, and $p \mid |K|$, then $\exists$ a Sylow p-subgroup H of K s.t. $H \cap K$ is a Sylow p-subgroup of K.

Applications:

· groups of order pq ($p < q$ are primes) ($n_q(G) = 1$)

· groups of order 12

5. Conjugacy in S_n

any element of S_n can be decomposed into disjoint cycles.

$$\sigma \in S_n \Rightarrow \sigma = (a_{1_1} \cdots a_{1_{\ell_1}}) \cdots (a_{k_1} \cdots a_{k_{\ell_k}})$$

· conjugation by $\tau \in S_n$

$$\tau \sigma \tau^{-1} = (\tau(a_{1_1}) \cdots \tau(a_{1_{\ell_1}})) \cdots (\tau(a_{k_1}) \cdots \tau(a_{k_{\ell_k}}))$$

6. Rings

· $(R, +)$ is an abelian group with identity 0
- multiplication $\times$ is associative with identity 1
· distributivity of $\times$ and $+$
· we generally assume commutativity of $\times$
· homomorphisms $(+, \times, 1)$
- ideals $I \subset R$
  - subgroups of $(R, +)$
  - $\forall\, x \in I,\ r \in R,\ rx \in I$

facts: – the kernel of any ring homomorphism is an ideal
– quotient construction $\Rightarrow$ every ideal I is the kernel of the ring homomorphism $R \to \bar{R} = R/I$

principal ideals: $(a) = \{ra \mid r \in R\}$

prop: let R be a commutative ring. Then R is a field $\Leftrightarrow$ R has exactly two ideals, namely $(0) = \{0\}$ and $(1) = R$.

when are ideals principal?

Euclidean algorithm $\Rightarrow$ every ideal of $\mathbb{Z}$ is principal.
F is a field $\Rightarrow$ Euclidean algorithm for $F[x] = \{$polynomials with coefficients in $F\}$ $\Rightarrow$ every ideal in $F[x]$ is principal.

ideals of quotients. Fix an ideal $I \subset R$. Then there is a correspondance

$$\left\{\begin{matrix}\text{ideals of}\\ \bar{R} = R/I\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{ideals } J \subset R\\ \text{containing } I\end{matrix}\right\}$$

$$\bar{J} \longmapsto f^{-1}(\bar{J})$$
$$f(J) \longleftarrow J \qquad // f: R \to R/I = \bar{R}$$

· $R/J \xrightarrow{\sim} \bar{R}/\bar{J}$ (induced by $R \to \bar{R} = R/I \to \bar{R}/\bar{J}$)

very simple example of creating relations:

prop: let F be a field. Then $F[x]/(x) \xrightarrow{\sim} F$

pf: $\varphi: F[x] \to F$, $P(x) \mapsto P(0)$ ring homomorphism. φ is surjective, so by the first isomorphism thm $F[x]/\ker\varphi \cong F$
$\varphi(P) = 0 \Leftrightarrow 0$ is a root of $P(x) \Leftrightarrow P(x) = xQ(x) \Leftrightarrow P(x) \in (x)$.
So $\ker\varphi = (x)$