Groups + Rings Review

Groups $G, *$ with associativity, identity + inverses.

Examples $(\mathbb{R},+)$ $(\mathbb{Z},+)$, $(\mathbb{R}^\times, \cdot)$. ___ _ _

- cyclic group $\mathbb{Z}_n = \{0,\dots,n-1\} = \mathbb{Z}/n\mathbb{Z}$
  $* = +_n$
- finite abelian group: classification $G \cong \mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \dots \times \mathbb{Z}_{p_k^{n_k}}$
  prime powers
  p_i's not necessarily distinct $\mathbb{Z}_4 \not\cong \mathbb{Z}_2 \times \mathbb{Z}_2$
- Symmetric group
  $S_n = \{ \sigma : \{1,\dots,n\} \to \{1,\dots,n\} \text{ bijections} \}$
  Cayley's Thm $\forall$ group G is isomorphic to a subgroup of S_G

Groups act on sets $*: G \times X \to X$

1) $e * x = x \quad \forall x \in X$

2) $h*(g*x) = (hg)*x \quad \forall x \in X \quad g,h \in G$

- Symmetric group S_n acts on $X = \{1, \dots, n\}$ (by definition)

$\sigma * i := \sigma(i)$

- G acts on itself in different ways.

example left multiplication
$$G \times G \to G$$
$$(g, h) \mapsto gh$$

conjugation :
$$G \times G \mapsto G$$
$$(g, h) \mapsto ghg^{-1}$$

- K is the splitting field of of irreducible $f(x) \in F[x]$

$G(K/F)$ acts on the set of zeros of $f(x)$

$Z = \{r_1, \dots, r_d\}$.

$\sigma \in G(K/F)$ then $\sigma(r_i) = r_j$ and σ gives an element of $S_Z \cong S_d$. So we can think of $G(K/F) \leq S_d$.

<u>Question</u> Why isn't every permutation of the roots possible?

We can sent any r_i to any r_j by extending the conjugation isomorphism $\Phi : F(r_i) \to F(r_j)$ but this may determine where some of the other roots go.

<u>Example</u> p-th cyclotomic extensions. $p = 5$ $\xi = e^{\frac{2\pi i}{5}}$ $\sigma(\xi)$ determines the images of all other roots of unity

$f(x) = x^4 + x^3 + x^2 + x + 1$

G acting on X $|G|, |X| < \infty$.

Orbit of $x \in X$ $\quad \mathcal{O}_x = \{x' \in X \mid gx = x' \ \exists g \in G\} \subseteq X$

$\mathcal{O}_x = \mathcal{O}_y \iff \exists g$ s.t. $gx = y$.

$X = \bigsqcup \mathcal{O}_i$ ← partition into disjoint orbits.

Burnside's Formula $\quad \#\text{orbits} = \dfrac{1}{|G|} \sum_{g \in G} |X_g|$ $\quad |G| < \infty$.

$X_g = \{x \in X \mid gx = x\} \subseteq X$

$X = \bigsqcup \mathcal{O}_i \Rightarrow |X| = \sum |\mathcal{O}_i|$. and $|\mathcal{O}_x| = (G : G_x)$

disjoint orbits

where $G_x = \{g \in G \mid gx = x\}$

Stabiliser subgroup of X.

Subgroups of groups $H \leq G$. (Galois correspondence)

Lagrange's Thm $|G| < \infty$ if $H \leq G$ then $|H|$ divides $|G|$

$\Rightarrow$ $\mathrm{ord}(a) = |\langle a \rangle|$ divide $|G|$ $\forall$ $a \in G$.

$\Rightarrow$ if $|G| = p$ prime no non-trivial subgroups.

Cosets of H: $eH, a_1H, \ldots, a_kH$ list disjoint cosets $|a_iH| = |a_jH| = |H|$

$G = \sqcup a_iH \cup H$

Normal subgroups $N \leq G$ s.t. $gNg^{-1} = N$ $\forall g \in G$.

N normal in G $\Leftrightarrow$ G/N $\{eN, a_1N, \ldots\}$ form a group with operation

$a_1Na_2N := a_1a_2N$

Review of : G

Centraliser (oblig #1) $\underset{\text{set}}{A} \subseteq G$ $\quad C(A) = \{g \in G \mid gag^{-1} = a \ \forall a \in A\}$

subgroup of G.

Center of G $= C(G) = \{g \in G \mid ghg^{-1} = h \ \forall h \in G\}$.

Normalizer of $H < G$ $\quad N(H) = \{g \in G \mid ghg^{-1} \in H \ \forall h \in H\}$

check text
book notation

H normal in $G \iff N(H) = G$.

Kernel $\quad \underset{*}{G} \xrightarrow{\phi} \underset{*'}{G'}$ $\quad$ group homomorphism $\phi(g_1 * g_2) = \phi(g_1) *' \phi(g_2)$

$\mathrm{Ker}(\phi) = \{g \in G \mid \phi(g) = e'\} \trianglelefteq G$.

$= \phi^{-1}\{e'\}$.

Proposition $\phi: G \to G'$ homomorphism is injective $\iff \mathrm{Ker}(\phi) = \{e\}$.

Sylow's Thms $|G| = p^n m$ $p \nmid m$ $n \geq 1$

1) a) G contains a subgroup of order p^i $\forall$ $1 \leq i \leq n$ existence of subgps of size prime powers

b) $H < G$ $|H| = p^i$ $i < n$ then $H \triangleleft H'$

2) If P_1, P_2 are p-Sylow subgroups $(|P_i| = p^n)$ then

$P_1 = g P g^{-1}$ for some $g \in G$ related by conjugation

3) $n_p = \#$ p-Sylow subgroups $n_p \equiv 1 \bmod p$ and

$n_p \mid |G|$

(If $n_p = 1$ then P p-Sylow group is normal) How many p-Sylow subgroups?

Exam 2009 Problem 1

1a) Find all abelian groups of order 63 up to isom.
Determine the subgroups of the cyclic one.

$63 = 3^2 \times 7$. By classification of finite abelian groups

$$G \cong \mathbb{Z}_{p_1^{n_1}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}}$$

so there are two $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_7$ or

$\mathbb{Z}_9 \times \mathbb{Z}_7 \cong \mathbb{Z}_{63}$ ← cyclic

$$\boxed{\begin{array}{c} \mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm} \\ \Updownarrow \ \gcd(n,m) = 1 \end{array}}$$

$\{0\}$, $\langle 21 \rangle$, $\langle 9 \rangle$, $\langle 7 \rangle$, $\langle 3 \rangle$, $\mathbb{Z}_{63}$

size: 1, 3, 7, 9, 21

1b Let G be non abelian of order 21. What are the possible orders of elts of G?

Find # Sylow p-subgroups of G $\forall$ p prime.

Determine how many elts G has of each order?

Does G have any other proper normal subgroups?

Solution

By Lagrange possible orders of elts and subgroups divide 21 hence 1, 3, 7 or 21.

Sylow subgroups are of size 3 or 7.

$\underline{21 = 3 \cdot 7}$ $n_7 \equiv 1 \mod 7 \Rightarrow n_7 = 1, 8, 15, \ldots$

$n_7 \mid 21 \Rightarrow n_7 = 1 \Rightarrow H_7$ the unique 7-Sylow subgroup is normal in G

$n_3 \equiv 1 \mod 3 \Rightarrow n_3 = \boxed{1}, 4, \boxed{7}, 10, 13, \ldots$

and $n_3 \mid 21$

Suppose $n_3 = 1 \Rightarrow H_3$ the unique 3-Sylow subgroup is normal in G.

Consider $\forall a, b \in G$ $aba^{-1}b^{-1}$ and show if H_3, H_7 are normal $aba^{-1}b^{-1} = 1$ and G is abelian

$\Leftarrow\!\!\!\!\!\times$ Hence $n_3 = 7$.

Rings $R, +, \cdot$ $(R,+)$ abelian group with multiplication $\cdot$

If $\cdot$ commutative $\to$ R commutative

If $\exists$ 1 identity for $\cdot$ $\Rightarrow$ R has unity.

Examples $\cdot$ $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Z}_n, +, \cdot)$ $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$. matrices, ...

- $F[x]$ polynomials with coefficients in a field F.

Ideals

R commutative: $I \subseteq R$ s.t. $(I, +)$ is a group and $\forall$ $r \in R$ $rI \subseteq I$. $\Rightarrow$ R/I ring of cosets is well defined.

Can quotient by ideals to get a new ring!

R commutative ring with unity $\quad R/I$ is a field $\iff$ I is maximal

$\Downarrow$

is an integral domain $\iff$ I is prime.

I is a prime ideal if whenever $ab \in I$ then either a or b is in I.

Example $R = \mathbb{Z} \quad I = \langle p \rangle = \{kp \mid k \in R\}$.

p prime number $\quad$ I is a prime ideal (also maximal!)

$\mathbb{Z}/\langle p \rangle \cong \mathbb{Z}_p$ in

$I \subseteq R$ is a principal ideal if $\exists\, a \in R$ s.t.

$$I = \langle a \rangle = \{ ra \mid r \in R \}.$$

<u>Recall</u> $R = F[x]$ then every ideal I is principal. (Proof via division alg.).

<u>Problem 3</u> <u>2009</u>