Group Theory

- proposition 1: $\mathbb{Z}/n\mathbb{Z}$ has exactly n elements
- proposition 2: Addition is correctly defined on $\mathbb{Z}/n\mathbb{Z}$, the class $[a]+[b]=[a+b]$ is the same for different elements of $[a]$ and $[b]$

  proof. $a_1, a_2 \in [a]$ $b_1, b_2 \in [b]$.

  $[a_1+b_1]=[a_2+b_2] \Leftrightarrow a_1+b_1 \sim a_2+b_2$

  $\Leftrightarrow n \mid a_1-a_2+b_1-b_2$
- proposition 3: Identity element e is always unique in any group G
- proposition3.18: G is a group. The inverse (a^{-1}) is unique
- proposition3.19: For any $a, b \in G$. $(a\cdot b)^{-1}=b^{-1}a^{-1}$
- Proposition3.20: $\forall g \in G.\ (g^{-1})^{-1}=g$
- Proposition3.22: $\forall a, b \in G$. if $ac=bc$ then $a=b$; if $ca=cb$ then $a=b$
- Proposition 3.30: $H \subseteq G$ is a subgroup of G iff
  1) (identity) $e_G \in H$
  2) (closure of the group operation) if $h_1, h_2 \in H$. then $h_1 * h_2 \in H$
  3) (closure of inverses) if $h \in G$. then $h^{-1} \in H$
- Lemma: $\langle a \rangle$ is a subgroup of G.
- Proposition: G is cyclic iff $\exists g \in G$. $G=\langle g \rangle$
- proposition: $\phi: G \to H$. G are groups and they are homomorphism. then
  1. $\phi(e_G)=e_H$
  2. $\phi(g)^{-1}=\phi(g^{-1})$
  3. if $k \leq G$. then $\phi(k) \leq H$

Group Theory

3'. as $G \leq G$. then $\phi(G) \leq H$

4. if $M \leq H$. then $\phi^{-1}(M) = g \in G$.
$\phi(g) \in M$ is a subgroup of G.

• Lemma 6.2

The following are equivalent

→ $g_1H = g_2H$ → $g_2 \in g_1H$

→ $Hg_1^{-1} = Hg_2^{-1}$ → $g_1^{-1}g_2 \in H$

→ $g_1H \subset g_2H$

• Corollary

If G is abelian, then every subgroup is normal

• Theorem

$\langle a \rangle$ is a subgroup and it's minimal subgroup $H \leq G$ s.t. $a \in H$

• Theorem

Every cyclic group is abelian
$\forall a, b \in G.\ a * b = b * a$

• Theorem 6.4
H-cosets partition G

We can find g_i: a set of elements of G such that $G = g_1H \cup g_2H \cup \cdots$ that $g_iH \cap g_jH = \phi$

• Theorem 6.10
Lagrange's Theorem

G = finite group. $H \leq G$.
$|G| = |H| \cdot |G/H|$

• Corollary 6.11

$g \in G$. $|g| \mid |G|$

• Theorem 9.7
+ Theorem 9.8

If G is a cyclic group. then

→ if it is finite order.
then it is isomorphic to $\mathbb{Z}/n\mathbb{Z}$

→ if it is of infinite order.
then it is isomorphic to $\mathbb{Z}$.

• Theorem / Proposition

if $G \neq H$ are isomorphic / finite / cyclic. then the other is

• First Isomorphism Theorem

If $\phi: G \to H$ is a homomorphism.
then $\mathrm{Im}(\phi) \cong G/\ker(\phi)$

• Theorem

If G is internal direct product of H and K. then $G \cong H \times K$

Group Theory

- proposition
- proposition

$\mathrm{Stab}_G(x) \leq G$.

= "G acts on X" by bijections: if you fix any $g \in G$: $\Phi(g, -)$ is a bijection of X

: "G acts on X" is almost the same as $G \leq \mathrm{Sym}(X)$. if $\Phi: G \times X \to X$ s.t. 1 and 2. then $\varphi: G \to \mathrm{Sym}(X)$, $g \mapsto \Phi(g, -)$ is a homomorphism.

- Orbit-Stabilizer Theorem

if G is finite, $|G| = |\mathrm{Stab}_G(x)||\mathrm{Orb}_G(x)|$

- Cayley's Theorem

Every group is isomorphic to a group of permutations.

- Burnside's Lemma.

G is a finite group. X is a finite set, G acts on X
Then number of G-orbits on X
$= \frac{1}{|G|} \sum_{g \in G} |X_g|$. where $X_g \subseteq X$

$X_g = \{x \in X \mid g(x) = x\}$.

Ring Theory

- proposition: ∀ ring R, $R^\times \cap \text{ZeroDiv}(R) = \phi$
- proposition: R = Units of $R \amalg \text{ZeroDiv}(R) \amalg$ else
- Prop 16.15: If $a \notin \text{ZeroDiv}(R)$, then $ab = ac \Rightarrow b = c$
- Theorem 16.16: R is finite and integral domain, then R is field.
- Proposition: $\{\ker f : f: G \to H\}$ group.
  $= \{\text{normal subgroups of } G\}$.
  $\{\ker \phi : \phi: R \to S\}$ ring
  $= \{\text{ideals of } R\}$.
- Proposition: R is a field ($R^\times = R \setminus \{0_R\}$), then the only ideals in R are $(0) = 0_R$ and R
- Theorem 16.35: R is a commutative ring with 1_R. $I \trianglelefteq R$, R/I is a field iff I is a maximal ideal in R.
- Second Isomorphism Theorem: if $I \trianglelefteq R$. $J \trianglelefteq R$. s.t. $I \subseteq J \trianglelefteq R$. then $J/I \trianglelefteq R/I$
- proposition: $(3) = 3\mathbb{Z} \trianglelefteq \mathbb{Z}$ is maximal
- Lemma: S is an integral domain iff (0) is a prime ideal.
- Theorem 16.38: R = commutative ring with 1_R. $I \trianglelefteq R$. then R/I is integral domain $\Leftrightarrow$ I is prime.
- Corollary: Every maximal ideal is prime. However, in general, maximal ideals of $R \subsetneq$ prime ideals of R
- proposition: a. $\langle x_1 \cdots x_k \rangle$ is an ideal
  b. $\langle x_1 \cdots x_k \rangle$ is a minimal ideal I such that $x_1 \in I, \cdots x_k \in I$

Ring Theory

- Proposition

1. $\langle x \rangle \cdot \langle y \rangle = \langle xy \rangle$
2. $\{0_R\} = \langle 0 \rangle \cdot I = \langle 0 \rangle$
3. $\langle 1_R \rangle \cdot I = I$

- Fundamental Theorem of Ideal Theory

$\forall$ ideal $I \trianglelefteq \mathbb{Z}[-\sqrt{-5}]$. $\exists a_1 a_2 \cdots a_m$:
$I = P_1^{a_1} P_2^{a_2} \cdots P_m^{a_m}$ for P_i are prime ideals

$\forall (n) \trianglelefteq \mathbb{Z}$, $\exists a$, s.t.
$(n) = (P_1)^{a_1} (P_2)^{a_2} \cdots (P_m)^{a_m}$, (P_i) are prime ideals.

- proposition

Let R be a ring. then every ideal $I \neq R$ is contained in a maximal ideal of R.

- proposition

let I be a subset of R. R is the kernel of a homomorphism iff I is an ideal

- proposition

If R is a division ring. then it is simple.

- proposition

A commutative Ring with $e \neq 0$ is simple iff it is a field.

- proposition

A proper ideal $(f) \subset F[x]$ is a non-zero prime ideal iff f is irreducible.

Field Theory

- Lemma: K/F is a field extension, then K is a vector space over F
- Theorem 21.17: $F \subseteq E \subseteq K$, $[K:F] = [K:E][E:F]$.
- Lemma: $L_{a(x)}$ is a linear map of E-vector space
- Lemma: $L_{a(x)}$ is invertible
- proposition: $\mathbb{Q}[\sqrt[3]{2}, \sqrt[4]{4}] \cong \mathbb{Q}[x]/(x^3-2)$
- Theorem: F is a field. $f(x) \in F$ is irreducible, then $F(x)/(f(x))$ is a field.