Up to Ch 10 in notes

Groups, Rings and Modules IB Lent

1 Group Theory

- Automorphism: Isomorphism from a group to itself
- A group G is a permutation group of degree n if $G \leq \mathrm{Sym}(X)$ for some set X with $|X| = n$

Isomorphism Theorems

- First Isomorphism Theorem:
  If H and G are groups and $\phi : H \to G$ a homomorphism, then
  $$H/\operatorname{Ker}\phi \cong \operatorname{Im}\phi$$
- Second Isomorphism Theorem:
  If $H \leq G, K \triangleleft G$, then $HK \leq G$, and $H \cap K \triangleleft H$, and
  $$\frac{H}{H \cap K} \cong \frac{HK}{K}$$
  (Use homomorphism $H \to HK/K$ by $h \mapsto hK$)
- Correspondence Theorem:
  If $K \triangleleft G$, then there exists bijection between
  $$\{\text{subgroups of } G \text{ containing } K\} \leftrightarrow \{\text{subgroups of } G/K\}$$
  $$\text{via} \qquad H \mapsto H/K$$
  $$\{g \in G : gK \in S\} \leftarrow\!\shortmid S$$
  This restricts to normal subgroups
- Third Isomorphism Theorem:
  If $K \leq H \leq G$ and $K \triangleleft G, H \triangleleft G$, then
  $$\frac{G/K}{H/K} \cong G/H$$
  (Use homomorphism $G/K \to G/H$ by $gK \mapsto gL$)

Simple Groups

A group G is simple iff its only normal subgroups are $\{e\}$ and G

- An abelian group is simple iff it is isomorphic to C_p, some prime p

  (Only if: any non-trivial g generates the whole group, so cyclic; not prime order $\implies$ have proper subgroup)

- If G is a finite group, then it has a composition series:

$$1 \lhd G_0 \lhd G_1 \lhd \cdots \lhd G_n = G,$$

  with each quotient group G_n/G_{n-1} simple.

  (Use correspondence theorem and induction)

Group Action

- An action of G on set X gives a permutation representation $\phi : G \to \mathrm{Sym}(X)$

- Examples:

  - G acts on itself/collection of cosets G/H by multiplication
  - Acts on itself/any normal subgroup by conjugation
  - G act on $\mathrm{Sub}(G)$, the set of its subgroups by conjugation

$$g * H = gHg^{-1}$$

    Stabiliser $= N_G(H) = \{g \in G : gHg^{-1} = H\}$, the normaliser of H in G
    $N_G(H)$ is the largest subgroup of G containing H as a normal subgroup

- If G is a non-abelian simple group, and $H \leq G$ of index $n > 1$. Then $n \geq 5$ and G is isomorphic to a subgroup of A_n

  (G acts on G/H by left mult, get injective hom $\implies$ $G \leq S_n$;
  $G \cap A_n \lhd G$, but $G \cap A_n = \{e\}$ $\implies$ $|G| = 2$, abelian)

Alternating Groups

Conjugacy class of g splits from S_n to A_n iff $\exists$ odd permutation that commutes with g

- A_n is simple for $n \geq 5$
  - A_n is generated by 3-cycles
    (3-cycles generate double transpositions, which generate A_n)
  - All 3-cycles are conjugate in A_n
  - Any non-trivial $N \triangleleft A_n$ contains a 3-cycle
    (consider cases)

p-groups

For a prime p, a finite group G is a p-group if $|G| = p^n$, some $n \in \mathbb{N}$

- p-groups have $Z \neq \{e\}$ (proof by counting)
- only simple p-group is C_p
- If G is a p-group of order p^n, then G has a subgroup of order p^r for $r = 0, 1, \ldots n$ (composition series)
- If $G/Z(G)$ is cyclic, then G is abelian (all elements have the form $g^i z$)

Sylow Theorems

Let G be a finite group of order $p^a m$, where p is a prime and $p \nmid m$. Then

1. $\mathrm{Syl}_p(G) = \{P \leq G : |P| = p^a\}$ is non-empty, i.e. there exists a Sylow p-subgroup
2. All elements of $\mathrm{Syl}_p(G)$ are conjugate
3. The number of Sylow p-subgroups $n_p = \left|\mathrm{Syl}_p(G)\right|$ satisfies

$$n_p \equiv 1 \pmod{p}, \text{ and } n_p \mid |G| \implies n_p \mid m$$

Matrix Groups

Over a field F, e.g. $\mathbb{C}, \mathbb{Z}/p\mathbb{Z}$, can have $GL_n(F)$, $SL_n(F)$, $PSL_n(F) = SL_n(F)/Z \cap SL_n(F)$, where $Z =$ center of $GL_n(F) =$ scalar matrices

Abelian Groups

- Decomposition: Every finite abelian group is isomorphic to product of cyclic groups (proof later in course)
- If m and n are coprime, then $C_n \times C_m \cong C_{mn}$
- If G is a finite abelian group, then $G \cong C_{p_1^{\alpha_1}} \times C_{p_2^{\alpha_2}} \times \dots C_{p_k^{\alpha_k}}$, where p_i are prime, not necessarily distinct OR $G \cong C_{d_1} \times C_{d_2} \times \dots C_{d_t}$, with $d_1 \mid d_2 \mid \cdots \mid d_t$

2 Ring Theory

- Definition:
  A ring is a triple $(R, +, \cdot)$, two binary operations (need to check closure), with axioms:
  - $(R, +)$ is an abelian group with identity 0
  - Multiplication is associative, and has identity 1
  - Distributivity: $(x + y) \cdot z = x \cdot z + y \cdot z, \quad x \cdot (y + z) = x \cdot y + x \cdot z$
- R is commutative if multiplication is commutative (addition automatically is)
  (All rings in GRM are commutative)
- Subring: $S \subseteq R$ is a subring (written $S \leq R$) if $(S, +, \cdot)$ is a ring, (thus must have same identity elements as R)
- An element $r \in R$ is a unit if it has a multiplicative inverse, units form a group under multiplication
- A field is a ring with $0 \neq 1$ and all non-zero elements are units

New rings from old

- Take product of rings, elementwise add/mult
- If R is a ring, X is a set, take the set of all functions $X \to R$ with pointwise operations:

$$(f+g)(x) = f(x) + g(x), \quad (f \cdot g)(x) = f(x) \cdot g(x)$$

- $R[X] = \{(a_0, a_1, \dots) \mid a_i \in R, \text{ finitely many non-zero}\}$
(Ring of polynomials with coeffs in R)

  Operations defined as polynomials: $(a_0, a_1, \dots, a_m, 0, \dots) = a_0 + a_1 X + \dots + a_m X^m$

  - Polys are different from functions (esp. in rings like $\mathbb{Z}/p\mathbb{Z}$)
  - Degree of polynomial $(a_0, a_1, \dots)$: largest m s.t. $a_m \neq 0$
  - Monic polynomial: degree m and $a_m = 1$
  - Division algorithm, induction

Examples:

- $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$
- Gaussian Integers $= \mathbb{Z}[i] = \{a + bi \mid a, b, \in \mathbb{Z}\}$
- $R[X_1, \dots X_n] = \{\text{polys in } X_1, ..., X_n \text{ with coefficients in } R\}$
- Power series $R[[X]]$ (convergence not an issue)
- Laurent polynomials $R[X, X^{-1}]$
- Zero ring: $\{0\}$, the only ring where $0 = 1$

Ideals, Quotients

- Ring homomorphism: $\phi : R \to S$ is a ring homomorphism if $\forall x, y \in R$
  - $\phi(x + y) = \phi(x) + \phi(y)$
  - $\phi(xy) = \phi(x)\phi(y)$

  - $\phi(1_R) = 1_S$

  (preserves structure of both $+$ and $\cdot$, need to specify image of 1 since elements need not have multiplicative inverse)

- Isomorphism = bijective homomorphism
- $\ker\phi = \{r \in R \mid \phi(r) = 0\}$
- $I \subseteq R$ is an ideal ($I \lhd R$) if
  - (Additive closure) I is a (normal, as addition must be commutative) subgroup of $(R, +)$
  - (Strong closure) If $r \in R$ and $x \in I$, then $rx \in I$
- An ideal I is a proper ideal if $I \neq R$ (I must not contain any unit)
  (In particular does not contain 1, so proper ideals are not subrings)
- If $\phi : R \to S$ is a homomorphism, then $\ker\phi \lhd R$
- Ideal generated by $a_1, a_2, \ldots a_n$:

$$(a_1, a_2, \ldots, a_n) = \{a_1 r_1 + a_2 r_2 + \cdots + a_n r_n \mid r_i \in R\}$$

  In particular, $(a) = aR = \{ar \mid r \in R\}$

- An ideal I is principal if $I = (a)$ for some a
- Quotient ring:
  If $I \lhd R$, then the set R/I of additive cosets of I form the quotient ring with operations:

$$\begin{aligned}(r_1 + I) + (r_2 + I) &= r_1 + r_2 + I \\ (r_1 + I) \cdot (r_2 + I) &= r_1 r_2 + I\end{aligned}$$

- I is an ideal $\iff$ I is a kernel of some homomorphism/quotient map
- There exist unique ring homomorphism $\phi : \mathbb{Z} \to R$:

$$1 \mapsto 1_R, \quad \pm n \mapsto \pm(\underbrace{1_R + \cdots + 1_R}_{n})$$

  $\ker\phi = n\mathbb{Z}$ for some $n = \operatorname{char} R \geq 0$, the characteristic of R
  (If $\operatorname{char} R > 0$, it is the order of 1_R in $(R, +)$; otherwise 1_R has infinite order)

Isomorphism Theorems

- First Isomorphism Theorem:
  If $\phi : R \to S$ is a ring homomorphism, then
  $$R/\operatorname{Ker}\phi \cong \operatorname{Im}\phi \leq S$$
- Second Isomorphism Theorem:
  Let $R \leq S, J \lhd S$, then $R \cap J \lhd R$, and $R + J \leq S$, and
  $$\frac{R}{R \cap J} \cong \frac{R + J}{J}$$
- Correspondence Theorem:
  If $I \lhd R$, then there exists bijection between
  $$\begin{gathered}\{\text{ideals in } R \text{ containing } I\} \leftrightarrow \{\text{ideals in } R/I\} \\ \text{via} \qquad J \mapsto J/I \\ \{r \in R : r + I \in K\} \leftarrow\!\shortmid K\end{gathered}$$
- Third Isomorphism Theorem:
  If $I \lhd R, J \lhd R$ and $I \subseteq J$, then $J/I \lhd R/I$ and
  $$\frac{R/I}{J/I} \cong R/J$$

Integral domain, maximal, prime ideals

- R (non-zero) is an integral domain if $\forall a, b \in R : ab = 0 \implies a = 0$ or $b = 0$
  i.e. no zero divisors ($a \neq 0$ is a zerodivisor if $\exists\, b \neq 0$ s.t. $ab = 0$)
- Finite integral domains are fields; all fields are integral domains
- R integral domain $\implies R[X]$ integral domain (polys with coeff in R)
- At most deg(f) many roots
- Any finite subgroup of the multiplicative group of a field is cyclic
- If R integral domain, there exists F field of fractions s.t.
  1. $R \leq F$

2. Every element of F may be written as ab^{-1}, for $a, b \in R$, $b \neq 0$ (b^{-1} is multiplicative inverse in F)

(via equivalence classes)

Look at rings only through its ideals:

- R a field $\iff$ only ideals are $\{0\}$ and R
- Maximal Ideal: $I \triangleleft R$ is maximal if for all ideal J with $I \leq J \leq R$, then $J = I$ or $J = R$ (no proper ideal strictly bigger R)
- $I \triangleleft R$ maximal $\iff$ R/I a field
- Prime Ideal: $I \triangleleft R$ is prime if $I \neq R$ and

$$\forall a, b, \in R : ab \in I \implies a \in I \text{ or } b \in I$$

- $I \triangleleft R$ prime $\iff$ R/I an integral domain
- Maximal ideal $\implies$ prime
- R integral domain, then $\operatorname{char} R = 0$ or prime number

Factorisation in rings

- Unit, divides, associates, irreducible (factorisation must contain a unit), prime ($p \mid ab \implies p \mid a$ or $p \mid b$) elements (also non-zero and not unit)
- (r) prime ideal $\iff$ r prime or $r = 0$
- Prime $\implies$ irreducible, converse false
- Principal Ideal Domain: every ideal is principal
- (r) maximal $\implies$ $r \in R$ is irreducible, converse holds if R is a PID
- Euclidean Domain (ED): there exists Euclidean function:

$$\phi : R \backslash \{0\} \to \mathbb{Z}_{\geq 0}$$

s.t.

(i) $a \mid b \implies \phi(a) \leq \phi(b)$

(ii) If $a, b \in R$ and $b \neq 0$, then $\exists\, q, r \in R$ with $a = qb + r$ and either $r = 0$ or $\phi(r) < \phi(b)$