Midterm 1 Review

Milan Capoor

10 Oct 2023

List of Topics

Groups:

1. Basic Definition
    - Symmetric Group
    - Permutation groups
    - Dihedral groups
    - Complex numbers
    - Cyclic groups
2. Subgroups
    - Cyclic Subgroups
    - Subgroups generated by a set
3. Homomorphisms
4. The Kernel
5. Cosets
6. Lagrange's Theorem
7. Euler's Theorem for $(\mathbb{Z}/n)^*$
8. RSA

Rings:

1. Basic definition
    - Matrices
    - Polynomials
    - $\mathbb{Z}/n$
    - Products
    -
2. Ideals
3. Homomorphisms
4. Group of units
5. Types of rings
    - Fields
    - Integral domains
6. Cosets
7. Quotient construction
8. Isomorphism theorem

Groups

Dihedral Group

Definition: the group of symmetries of regular polygons

Example:

- $D_3 = \{e, r, r^2, f, f^2, f^3\}$

Order: the order of D_n is $2n$

Subgroup: the subgroup of rotations of D_n are isomorphic to the cyclic group C_n and (equivalently) to $\mathbb{Z}/n$

Groups of prime order

Have no subgroups other than $\{e\}$ and G

Groups generated by multiple elements

$\langle g_1, \ldots, g_k \rangle = \{$all "words" in $g_1, \ldots, g_k$ and their inverses$\}$ = the intersection of all subgroups that contain $g_1, \ldots, g_k$

Cosets

$H \subset G$. Look at all aH

$$H \to aH, \quad h \mapsto ah$$

These provide a partition of the group by cosets of the same size.

We also know that all cosets are identical or disjoint.

Euler's Theorem

$$\phi(n) = \#(\mathbb{Z}/n\mathbb{Z})^*$$

where $(\mathbb{Z}/n\mathbb{Z})^*$ is the group of units (all the elements with inverses) of $\mathbb{Z}/n\mathbb{Z}$ which is the same as all the elements that are relatively prime to n.

Example: $(\mathbb{Z}/8)^* = \{1, 3, 5, 7\} \longrightarrow \phi(8) = 4$

By Lagrange's theorem, if $a \in (\mathbb{Z}/n\mathbb{Z})^*$ then $o(a) \Big| \phi(n)$ or $a^{\phi(n)/d} = 1$ in $(\mathbb{Z}/n\mathbb{Z})^*$. So

$$a^{\phi(n)} \equiv 1 \mod n$$

(if $\gcd(a, n) = 1$)

Rings

Ideal

For a commutative ring R, $I \subset R$ is an ideal when $(I, +)$ is an abelian subgroup and it has the **absorber property**

$$ar \in I, \qquad \forall a \in I, r \in R$$

Cosets: $\{a + I, a \in R\}$ *The only subgroup that is a coset is* $0 + I$

Homomorphism

A ring homomorphism is also a group homomorphism (because a ring is an "enhancement" of an abelian group)

The kernel of a group is a subgroup. The kernel of a ring is a subring, but more strongly, an ideal.

Group of units

Unit: an element in a ring with an inverse

Proof of group:

$$aa^{-1} = 1 \tag{1}$$
$$bb^{-1} = 1 \tag{2}$$
$$ab \cdot a^{-1}b^{-1} = 1 \tag{3}$$

Field: if every non-zero element is a unit

Quotient

Given an ideal I and ring R, R/I is the set of cosets $\{a + I,\ a \in R\}$ with

$$(a + I) + (b + I) = (a + b) + I$$
$$(a + I)(b + I) = (ab) + I$$

assuming that the above are well-defined.

The first formula comes from the fact I is a group. For the second, observe

$$a' = a + i_1 \quad b' = b + i_2 \tag{4}$$
$$a'b' = (a + i_1)(b + i_2) = ab + ai_2 + bi_2 + i_1 i_2 \tag{5}$$

And by the absorber property, all the products with i are in I so

$$a'b' = ab + I$$

so the cosets are the same.

Isomorphism theorem

We have a homomorphism $\phi : R_1 \to R_2$ which may or may not be onto. We also have

$$I = \ker(\phi) = \phi^{-1}(0) = \{r \in R_1 : \phi(r) = 0\}$$

$$\begin{tikzcd}
R_1 \arrow[r, "\pi"] \arrow[d, "\phi"'] & R_2 \arrow[dl, "\alpha"] \\
R_1/I &
\end{tikzcd}$$

By definition, $\alpha(a + I) = \phi(a)$

If $\alpha(a + I) = 0$, then $\phi(a) = 0$ so $a \in I \implies a + I = 0 + I$. This shows that the kernel is trivial so the map is injective.

Theorem: the map $\alpha : R_1/I \to R_2$ is a ring isomorphism

Generally, given R_1/I you guess an R_2 and look for a homomorphism from R_1 to R_2 which is onto and then compute the kernel.

Example 1: Show that $\mathbb{R}[x]/(x^2 + 1)R[x]$ is isomorphic to the complex numbers.

We find a typical member of $R_1 = \mathbb{R}[x]$:

$$\sum a_k x^k$$

And a typical member of $\mathbb{C} = \mathbb{R}[i]$

$$\sum a_k i^k$$

So

$$\phi : R_1 \to R_2 \qquad \sum a_k x^k \mapsto a_k i^k$$

This is onto because to get any value $a + bi$ we just need to see $a + bx$.

Then to calculate the kernel, notice

$$p(x) = a + bx + (x^2 + 1)q(x)$$

which is just the analog of the division algorithm.

We want this to be in the kernel so

$$0 = p(i) = a + bi + 0q(x)$$

which implies $a, b = 0$ so

$$p(x) = (x^2 + 1)q(x) = I$$

Example 2: $R_1 = \mathbb{Q}[x]$ and $I = \mathbb{Q}[x](x^2 - 5)$. What is R_1/I?

We notice that $x^2 - 5 = 0 \implies x = \sqrt{5}$ so we guess $\mathbb{Q}[\sqrt{5}]$. Now we want an onto ring homomorphism from $\mathbb{Q}[x] \to \mathbb{Q}[\sqrt{5}]$. So

$$\sum a_k x^k \to \sum a_k (\sqrt{5})^k$$

This is surjective because

$$a + bx \mapsto a + b\sqrt{5}$$

Then

$$p(x) = a + bx + (x^2 - 5)q(x)$$

so $p(x) = I$ when a and b are 0.