Lecture 21

Last time

- Defined **rings** $(R, +, \cdot)$:

$$\begin{cases} (R,+) \text{ is an abelian group,} \\ (R,\cdot) \text{ is a monoid,} \\ a(b+c) = ab + ac, \quad (b+c)a = ba + ca. \end{cases}$$

- Examples: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/n\mathbb{Z}, \mathrm{Mat}_{2\times 2}, \ldots$
- Defined **polynomial ring** $R[x]$ for an arbitrary ring R:

$$R[x] = \{a_0 + a_1 x + \cdots + a_n x^n \mid a_i \in R\}.$$

- Discussed **division with remainder** in $R[x]$:

$$f(x), h(x) \in R[x], \quad h(x) \text{ monic.}$$

Then there exist unique $q(x), r(x) \in R[x]$ such that

$$f(x) = q(x)h(x) + r(x), \quad \deg r(x) < \deg h(x).$$

Lemma

α is a **root** of $f(x)$ if and only if

$$f(x) = (x-\alpha)q(x) \text{ for some } q(x) \in R[x].$$

Proof. If $f(x) = (x-\alpha)q(x)$, then $f(\alpha) = (\alpha-\alpha)q(\alpha) = 0$.
Conversely, if $f(\alpha) = 0$, then divide $f(x)$ by $(x-\alpha)$:

$$f(x) = (x-\alpha)q(x) + r(x),$$

where $\deg r(x) < 1 \Rightarrow r(x) = r \in R$. Then $f(\alpha) = 0 = (\alpha-\alpha)q(\alpha) + r = r$, so $r = 0$. Hence $f(x) = (x-\alpha)q(x)$.

Definition

A ring R has **no zero divisors** if for all $a, b \in R \setminus \{0\}$,

$$ab \neq 0.$$

Examples: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

In general, if R is a division ring (in particular, a field), then R has no zero divisors.

Examples

$$\mathbb{Z}/6\mathbb{Z}: \quad 2 \cdot 3 = 0 \Rightarrow \text{has zero divisors.}$$

In general, if n is not prime, $\mathbb{Z}/n\mathbb{Z}$ has zero divisors.

Also, in $\mathrm{Mat}_{2\times 2}(\mathbb{R})$,

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \Rightarrow \text{zero divisors.}$$

Theorem

Assume R has no zero divisors (e.g., R is a field). For $f(x) \in R[x]$,

$$\#\text{roots of } f \leq \deg f.$$

Proof. By induction on $n = \deg f$. Induction step: pick any root α of f. By the lemma, $f(x) = (x - \alpha)q(x)$ with $\deg q = n - 1$.

Claim:

$$\{\text{roots of } f\} = \{\text{roots of } q\} \cup \{\alpha\}.$$

If $\beta \neq \alpha$ and $f(\beta) = 0$, then

$$f(\beta) = (\beta - \alpha)q(\beta) = 0 \Rightarrow q(\beta) = 0,$$

since R has no zero divisors. Hence the number of roots of f is at most

$$\#\text{roots of } f \leq \#\text{roots of } q + 1 \leq (n-1) + 1 = n.$$

Next time: use this theorem to prove that

$$(\mathbb{Z}/p\mathbb{Z})^\times \text{ is cyclic,}$$

and more generally, $R^\times$ is cyclic for any finite field R.

Monoid and Group Rings

Starting with an arbitrary monoid G and ring R, we can associate the ring

$$RG = \left\{ \sum_{i=1}^{n} r_i g_i \mid r_i \in R,\, g_i \in G \right\}.$$

If G is a group, this is called a **group ring**.

Define ring operations:

$$\left(\sum_i a_i g_i\right) + \left(\sum_i b_i g_i\right) = \sum_i (a_i + b_i) g_i,$$

$$\left(\sum_i a_i g_i\right)\left(\sum_j b_j g_j\right) = \sum_{g \in G} \left(\sum_{g_i g_j = g} a_i b_j \right) g.$$

Examples

$R[x]$ is a particular case of RG for $G = \mathbb{Z}_{\geq 0}$, since

$$R[x] = \{r_0 + r_1 x + \cdots + r_n x^n\},$$

and the product in $\mathbb{Z}_{\geq 0}$ corresponds to the product of monomials $x^m \cdot x^n = x^{m+n}$.

Example: Group Algebra

Let $G = D_8 = \langle r, s \mid r^4 = s^2 = 1, rs = sr^{-1} \rangle$. Then

$$G = \{r^k s^m \mid k = 1, 2, 3, 4;\ m = 0, 1\}.$$

Take $R = \mathbb{Z}$. Typical elements of $\mathbb{Z}D_8$ are:

$$\alpha = r + r^2 - 2s, \quad \beta = -3r^2 + rs.$$

Their sum and product:

$$\alpha + \beta = r - 2r^2 - 2s + rs,$$

$$\alpha\beta = -5r^3 - 3 + 7r^2 s + r^3 s.$$

Remark: We obtain many examples of noncommutative rings: if G is noncommutative and $R = \mathbb{Z}$, then $\mathbb{Z}G$ is noncommutative.

Embedding of Groups

If G is a group, then

$$G \subset (RG)^\times,$$

since for $g \in G$, its inverse in RG is g^{-1}.

Modules over a Ring

Analogous to group actions.

Definition. Let R be a ring. A **module over** R is a set M with:

1. an addition $+ : M \times M \to M$,
2. a scalar multiplication $\cdot : R \times M \to M$,

such that:

$$\begin{aligned} (M, +) &\text{ is an abelian group,} \\ (r + s) \cdot m &= r \cdot m + s \cdot m, \\ r \cdot (m + n) &= r \cdot m + r \cdot n, \\ (rs) \cdot m &= r \cdot (s \cdot m), \\ 1 \cdot m &= m, \quad \forall r, s \in R,\ m, n \in M. \end{aligned}$$

Example: $\mathbb{Z}$-modules are abelian groups.