Math 494

Yiwei Fu

1

Lase time: Defined a ring to be an abelian group under $+$ which has an associative operation $* : R \times R \to R$ with an identity element in R such that the distribution law holds.

Example 1.1. G is an abelian group under $+ \implies \mathrm{End}(G)$ is a ring under

$$(\phi + \psi)(g) := \phi(g) + \psi(g), \phi * \psi := \phi \circ \psi.$$

Definition 1.1. Suppose R, S are rings. A function $f : R \to S$ is a ring homomorphism if

$$f(r_1 + r_2) = f(r_1) + f(r_2), f(r_1 * r_2) = f(r_1) * f(r_2), f(1_R) = f(1_S)$$

Lemma 1.1. *If $f : R \to S$ is a ring homomorphism then $f(R)$ is a ring*

Definition 1.2. A <u>subring</u> of a ring R is a subset of R which is a ring under $+, *$ from R.

Definition 1.3. Suppose R, S are rings. An <u>isomorphism</u> $f : R \to S$ is a bijective homomorphism.

<u>NOTE</u>: The set-theoretic inverse $f^{-1} : S \to R$ is then a ring homomorphism.

Lemma 1.2. *R is a ring* $\implies r \cdot 0 = 0 \cdot r = 0,\ \forall r \in R.$

Proof.

$$0 + 0 = 0 \implies r \cdot (0 + 0) = r \cdot 0.$$ ■

Lemma 1.3.

$$(-1) \cdot r = -r = r \cdot (-1)$$

Proof.

$$1 + (-1) = 0 \implies (1 + (-1)) \cdot r = 0 \cdot r \implies r + (-1) \cdot r = 0$$ ■

It is always to check since we are so used to commutative things but it is not always the case.

Theorem 1.2. *Every ring is isomorphic to a subring of* $\mathrm{End}(G)$ *for some abelian group* G.

Proof. Let G be the additive group of R. For $r \in R$ define $[r] : G \to G, g \mapsto rg$. Check:

1. $[r] \in \mathrm{End}(G)$.

$$[r](g_1 + g_2) := r(g_1 + g_2) = rg_1 + rg_2 = ([r]g_1) + ([r]g_2).$$

2. $r \mapsto [r]$ is a ring homomorphism $R \to \mathrm{End}(G)$

$$[rs](g) = (rs)g = r(sg) = [r](sg) = [r]([s]g)$$

3. $r \mapsto [r]$ is injective

So $\phi : R \to \mathrm{End}(G), r \mapsto [r]$ is an injective ring homomorphism. Hence $\phi(R)$ is a subring of $\mathrm{End}(G)$ and $\phi : R \to \phi(R)$ is an isomorphism. ■

Definition 1.4. Suppose R is a ring and $r \in R$. Say $s \in R$ is a inverse of r if $rs = 1 = sr$. If r has an inverse then say r is a unit in R. Write R^* or $R^\times$ for the set of units in R.

<u>NOTE:</u> if s exists then it is unique:

$$rs = 1 = tr \implies (rs)s = (tr)s = t(rs) \implies s = t.$$

So we can denote s as r^{-1}.

<u>NOTE:</u> R^* is a group under multiplication.

Example 1.3. If G is a abelian group, then $(\mathrm{End}(G))^* = \mathrm{Aut}(G)$,

$$\mathrm{End}(\mathbb{Z} \text{ as a group}) \cong \mathbb{Z} \text{ as a ring},\ \mathrm{Aut}(\mathbb{Z} \text{ as a group}) = \{\pm 1\}.$$

$$\mathrm{End}(C_m) \cong \mathbb{Z}/m\mathbb{Z} \text{ as a ring},\ \mathrm{Aut}(C_m) = (\mathbb{Z}/m\mathbb{Z})^* = \{k \bmod m : \gcd(k, m) = 1\}.$$

$$\mathrm{Aut}(\mathbb{Z} \times \mathbb{Z} \text{ as a group}) \cong \mathrm{GL}_2(\mathbb{Z})$$

More rings: $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$. It turns out that all units are $\pm(1+\sqrt{2})^n,\ n \in \mathbb{Z}$.

Let R = ring of entire functions on $\mathbb{C}$ (power series which converge everywhere on $\mathbb{C}$). $R^* = \{\text{function in } R \text{ with no zeros}\} = \{e^{f(x)} : f(x) \in \mathbb{R}\}$.

An old but excellent result.

Theorem 1.4. *(Borel, 1893) If* $f_1, \ldots, f_n \in R^*$ *satisfy* $f_1 + \ldots + f_n = 0$ *but no (non-empty) proper subset of* $\{f_1, \ldots, f_n\}$ *sums to 0. then* $f_i/f_j \in \mathbb{C}^*, \forall i, j$.