Algebraic Theory I

Thomas Fleming

October 25, 2021

Contents

Lecture 25: Review of Test and Intro to Ring Theory

Fri 22 Oct 2021 11:31

Proof of question 6. Let $C_{105} \rtimes_\alpha C_5$ and define $\alpha : C_5 \to \text{Aut}\left(C_{105}\right)$. Recall, we need only show α is the trivial homomorphism. Recall $\text{Aut}\left(C_{105}\right) = C_2 \times C_4 \times C_6$. Hence, $\left|\text{Aut}\left(C_{105}\right)\right| = 2 \cdot 4 \cdot 6$ and as $5 \nmid 2 \cdot 4 \cdot 6$, we see every element must map to 1. $\square$

1 Intro to Ring Theory

Definition 1.1 (Ring)**.** A **ring** R is a set equipped with two closed operations $+$ and $\times$ obeying the following properties

1. $(R, +)$ forms an abelian group with additive identity, 0 .
2. There is a multiplicative identity, 1 .
3. $0 \neq 1$. (This would guarantee the ring is trivial)
4. The multiplicative operation is associative : $(xy)\, z = x\,(yz)$ for all $x, y, z \in R$.
5. The distributive properties hold: $x\,(y+z) = xy + xz$ and $(x+y)\,z = xz + yz$ for all $x, y, z \in R$.

A ring for which the multiplication operation is also commutative: $xy = yx$, will be called a **commutative ring**.
In general not every element $x \in R$ has a multiplicative inverse. We define the special class of elements with inverses the **units** of R and we denote x^{-1} to denote the unique inverse of a unit x.
A (not necessarily commutative) ring in which every nonzero element is a unit is a **division ring**. A commutative ring for which every nonzero element is a unit is a **field**.

Remark. Technically, a ring need not have a multiplicative identity, but almost all of them will be equipped with one. Sometimes we denote a ring without identity to be a rng (no i).

Example. ◇

Lecture 26: Ring Theory

Mon 25 Oct 2021 11:31

Recall. A ring is a set, an abelian addition and an associative multiplication with identity.

Definition 1.2 (Subring)**.** A **subring**, R' of R is a subset $R' \subseteq R$ such that R' is closed under its operations and $1 \in R'$.

This object turns out to be mostly uninteresting, so we introduce the following concept.

Definition 1.3 (Ideal)**.** A **left ideal** of the ring R is a nonempty subset $I \subseteq R$ so that $I \leq R$ under addition and $rI \subseteq I$ for all $r \in R$. This second condition is equivalent to for all $x \in I$, $r \in R \Rightarrow rx \in I$.
Right ideals follow the same first condition and for the second condition we have $Ir \subseteq I$ for all $r \in R$. A **(two-sided) ideal** is a set I which is both a left and a right ideal.

Example. $I = p\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

◇

Ideals will play a similar role as that of normal subgroups.

Definition 1.4 (Ring Homomorphisms)**.** If R, R' are rings and $\psi : R \to R'$ is a map. ψ is a **ring homomorphism** if

- $\psi(x + y) = \psi(x) + \psi(y)$ for all $x, y \in R$,
- $\psi(xy) = \psi(x)\psi(y)$ for all $x, y \in R$,
- $\psi(1_R) = 1_{R'}$ (if R, R' are rings with identities).

A ring homomorphism which is a bijection is a **ring isomorphism**.

Example. If $R = \mathbb{Z}/6\mathbb{Z}$. Consider the map $f : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$, $x \mapsto 3x$. We see the first two conditions hold under standard modular arithmetic, but the identity condition clearly fails, so we would consider this a ring homomorphism of rings without identity, but it is not a homomorphism of rings with identity.
◇

Definition 1.5. If R is a ring and $I \subseteq R$ is an ideal.
Then, we define $R/I = \{x + I : x \in R\}$, with $(x + I) + (y + I) := (x + y) + I$ and $(x + I)(y + I) := xy + I$, to be the **quotient ring** of $R \mod I$.

We see this operation to be well defined as $x' + I = x + I$ and $y' + I = x + I$ implies $x' + a = x$ and $y' + b = y$ for some $a, b \in I$, so we find $xy + I =$

$(x'+a)(y'+b)+I = x'y'+x'b+ay'+ab+I = x'y'+I$ by the absorption property.

Theorem 1.1 (1st Isomorphism Theorem for Rings)**.** If $\psi : R \to R'$ is a surjective ring homomorphism, then $\ker(\psi)$ is a two-sided ideal in R and $R/\ker(\psi) \simeq R'$.

Proof. First, we verify $\ker(\psi)$ is an ideal. It is clearly an additive subgroup as ψ is an additive group homomorphism. Also, if $x \in \ker(\psi)$ and $r \in R$, we see $\psi(x) = 0$, hence

$$\begin{aligned} \psi(rx) &= \psi(r)\psi(x) = 0 \\ \psi(xr) &= \psi(x)\psi(r) = 0 \\ &\Rightarrow rx, xr \in \ker(\psi). \end{aligned}$$

Hence, we find $\ker(\psi) = I$ is an ideal. Now, take the map We wish to show this is well-defined, so we must show that $\psi(x) = \psi(x')$ produces the same coset. As it turns out, this is in fact well defined, so we need only show there is a bijective homomorphism. Clearly the map is surjective and

$$\begin{aligned} xy &\mapsto xy+I \\ x &\mapsto x+I \\ y &\mapsto y+I \\ \text{and } (x+I)(y+I) = xy+I &\mapsto xy+I. \end{aligned}$$

Hence it is a homomorphism. Lastly, as this is an injective map at the group theory level, it is trivial to show injection holds. Hence $R' \simeq R/\ker(\psi)$. □

Remark. It has yet to be formally stated, but $0 \cdot x = 0$ for all $x \in R$ as $ax = ax$, hence $(a-a)x = 0$, so $0 \cdot x = 0$ (and $x \cdot 0 = 0$).

Definition 1.6. If R is a ring with $X \subseteq R$, then (X) is the smallest ideal containing X. In other words,

$$(X) = \bigcap_{\substack{X \subseteq I \subseteq R \\ I \text{ is an ideal}}} I.$$

Elements of (X) have the form $\sum_{i=1}^{n} \prod_{j=1}^{m} x_{j_i}$ for $x_i \in X$. That is, linear combinations of monomials with terms from X.

Remark. The intersection of (right/left/two-sided) ideals is itself a (right/left/two-sided) ideal.