LECTURE 7.

ALIREZA SALEHI GOLSEFIDY

Last time we define the factor ring R/I, where I is an ideal of R. We essentially defined the ring structure on R/I such that:

Corollary 1. *The map* $f : R \to R/I$, $f(x) := x + I$ *is a ring homomorphism and* $\ker(f) = I$.

Remark 2. Corollary 1 shows that there is a bijection between the set of all the ideals of R and the set of all the kernel of homomorphisms from R to any other ring.

Let us recall the following fact from group theory:

Lemma 3. *Let* I *be a subgroup of the abelian group* R*. Then*

$$x_1 + I = x_2 + I \Leftrightarrow x_1 - x_2 \in I.$$

Proof. Since $0 \in I$, $x_1 = x_1 + 0 \in x_1 + I = x_2 + I$. Hence there is $a \in I$ such that $x_1 = x_2 + a$. Thus $x_1 - x_2 = a \in I$.

On the other hand, if $x_1 - x_2 = a \in I$, then $x_1 + I = (x_2 + a) + I$. Since I is a group and $a \in I$, we have that $a + I = I$. Therefore $x_2 + a + I = x_2 + I$, which finishes our proof. □

Theorem 4. *Let* $f : R \to S$ *be a ring homomorphism. Then*

$$\overline{f} : R/\ker(f) \to \mathrm{Im}(f),\ \overline{f}(x + \ker(f)) := f(x)$$

is a ring isomorphism.

Proof. **Well-defined:** We have to show that if $x + \ker(f) = x' + \ker(f)$, then $f(x) = f(x')$.

$$\begin{aligned} x + \ker(f) = x' + \ker(f) &\Rightarrow x - x' \in \ker(f) \\ &\Rightarrow f(x - x') = 0 \\ &\Rightarrow f(x) = f(x'). \end{aligned}$$

Injective: We have to show that if $\overline{f}(x + \ker(f)) = \overline{f}(x' + \ker(f))$, then $x + \ker(f) = x' + \ker(f)$.

$$\begin{aligned} \overline{f}(x + \ker(f)) = \overline{f}(x' + \ker(f)) &\Rightarrow f(x) = f(x') \\ &\Rightarrow f(x - x') = 0 \\ &\Rightarrow x - x' \in \ker(f) \\ &\Rightarrow x + \ker(f) = x' + \ker(f). \end{aligned}$$

Surjective: We have to show $\mathrm{Im}(\overline{f}) = \mathrm{Im}(f)$.

Let $y \in \mathrm{Im}(f)$. Then by the definition, there is $x \in R$ such that $y = f(x)$. Hence $y = \overline{f}(x + \ker(f)) \in \mathrm{Im}(\overline{f})$.

Homomorphism: We have to show that $\overline{f}$ preserves the additive and the multiplicative structures. We just show the multiplicative case. The other one is similar.

Date: 1/25/2012.

$$\begin{aligned}\overline{f}((x+\ker(f))(y+\ker(f))) &= \overline{f}((xy)+\ker(f))\\ &= f(xy)\\ &= f(x)f(y)\\ &= \overline{f}(x+\ker(f))\overline{f}(y+\ker(f)).\end{aligned}$$

□

Definition 5. A ring S is called a homomorphic image of R if there is an onto ring homomorphism from R to S.

Corollary 6. *Any homomorphic image of R is isomorphic to a ring factor of R.*

Example 7. *Any ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some non-negative integer n. In particular, any homomorphic image of $\mathbb{Z}$ is isomorphic to either $\mathbb{Z}$, $\{0\}$ or $\mathbb{Z}/n\mathbb{Z}$ for some positive integer n.*

Definition 8. Let $X \subseteq R$. The ideal generated by X is the smallest ideal of R which contains X. It is denoted by $\langle X\rangle$. Since the intersection of a family of ideals is again an ideal, one can see that

$$\langle X\rangle = \bigcap_{I \lhd R,\ X\subseteq I} I.$$

Lemma 9. *Let R be a unital commutative ring and $X = \{a_1, \ldots, a_n\} \subseteq R$. Then*

$$\langle X\rangle = \langle a_1, \ldots, a_n\rangle = \{\sum_{i=1}^{n} r_i a_i |\ \forall\ i,\ r_i \in R\}.$$

Proof. X **is a subset of** I**:** Let $I = \{\sum_{i=1}^n r_i a_i |\ \forall\ i,\ r_i \in R\}$. Since R is a unital ring, for any i, $a_i = 1{\cdot}a_i \in I$. So $X \subseteq I$.

I **is an ideal:** We have to show (1) if $a, b \in I$, then $a - b \in I$, (2) if $a \in I$ and $r \in R$, then $ra \in I$. (Since R is commutative, we do not need to check if $ar \in I$.)

(1) $\sum_{i=1}^n r_i a_i - \sum_{i=1}^n r'_i a_i = \sum_{i=1}^n (r_i - r'_i)a_i \in I$.

(2) $r \cdot \sum_{i=1}^n r_i a_i = \sum_{i=1}^n (rr_i)a$.

I **is the smallest ideal which contains all the** a_i**'s:** Let J be an ideal of R and $X \subseteq J$. Then for any $r_i \in R$ we have that $r_i a_i \in J$ since J is an ideal. Thus $\sum_{i=1}^n r_i a_i \in J$ since J is closed under addition. Hence $I \subseteq J$. □

Example 10. *Any ideal in $\mathbb{Z}$ is generated by one element: $n\mathbb{Z} = \langle n\rangle$.*

Mathematics Dept, University of California, San Diego, CA 92093-0112

E-mail address: golsefidy@ucsd.edu