LECTURE 5.

ALIREZA SALEHI GOLSEFIDY

Last time we defined the characteristic of a ring.

Lemma 1. *Let R be an integral domain. Then* $\mathrm{char}(R)$ *is either a prime number or zero.*

Proof. If not, then $\mathrm{char}(R) = \mathrm{ord}(1)$ is a composite positive integer. Let $\mathrm{char}(R) = ab$ where $1 < a, b < \mathrm{char}(R)$. Then $(a1)(b1) = (ab)1 = 0$ and $a1 \neq 0$ and $b1 \neq 0$, which contradicts the fact that R has no zero-divisor. □

Remark 2. As I said earlier, whenever one would like to study a new structure in mathematics, one has to consider the maps from between these objects which preserve their structure. Such maps are called *homomorphism*.

Definition 3. Let R_1 and R_2 be two rings. A function $f : R_1 \to R_2$ is called a (ring) *homomorphism* if

(1) f is an additive group homomorphism, i.e. $f(a + b) = f(a) + f(b)$ and $f(-a) = -f(a)$.
(2) $f(ab) = f(a)f(b)$.

Remark 4. It is enough to check that $f(a - b) = f(a) - f(b)$ and $f(ab) = f(a)f(b)$.

Example 5. (1) *For any positive integer n, $f : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $f(x) := x + n\mathbb{Z}$ is a ring homomorphism.*
(2) *Let R be a unital ring. Then $f : \mathbb{Z} \to R$, $f(n) = n1_R$ is ring homomorphism.*

As you have seen in group theory, one can associate two new objects to a homomorphism: its image and its kernel.

Definition 6. Let $f : R_1 \to R_2$ be a ring homomorphism. Then the image of f is

$$\mathrm{Im}(f) := \{f(a) |\ a \in R_1\}$$

and its kernel is

$$\ker(f) := \{a \in R_1 |\ f(a) = 0\}.$$

Lemma 7. *Let $f : R_1 \to R_2$ be a ring homomorphism. Then*

(1) $\mathrm{Im}(f)$ *is a subring of R_2.*
(2) $\ker(f)$ *is a subring of R_1. Moreover for any $c \in R_1$ and b in* $\ker(f)$, *we have that* $cb \in \ker(f)$ *and* $bc \in \ker(f)$, *i.e.* $R_1 \ker(f) = \ker(f)R_1 = \ker(f)$.

Proof. 1. We have to check if $\mathrm{Im}(f)$ is closed under subtraction and multiplication: $f(a) - f(b) = f(a-b) \in \mathrm{Im}(f)$ and $f(a)f(b) = f(ab) \in \mathrm{Im}(f)$.

2. Let $a, b \in \ker(f)$; then $f(a - b) = f(a) - f(b) = 0 - 0 = 0$. So $a - b \in \ker(f)$. Let $c \in R_1$ and $b \in \ker(f)$; then $f(cb) = f(c)f(b) = f(c) \cdot 0 = 0$ and $f(bc) = f(b)f(c) = 0 \cdot f(c) = 0$. Hence $cb, bc \in \ker(f)$. □

It is a motivation to define the notion of an ideal:

Definition 8. A subset I of a ring R is called an it ideal of R if

Date: 1/20/2012.

(1) I is a subring.
(2) $RI = IR = I$, i.e. for any $r \in R$ and $a \in I$ we have $ra \in I$ and $ar \in I$.

Corollary 9. *Let $f : R_1 \to R_2$ be a ring homomorphism; then $\ker(f)$ is an ideal in R_1.*

Remark 10. Let $f : R_1 \to R_2$ be a ring homomorphism; then the image of f is NOT necessarily an ideal of R_2.

Example 11. (1) *$\{0\}$ and R are ideals of R.*
(2) *All the ideals of $\mathbb{Z}$ are of the form $n\mathbb{Z}$. (Any subring of $\mathbb{Z}$ is an ideal, too!)*
(3) *If I is an ideal of R and $I \cap U(R) \neq \varnothing$, then $I = R$.*
(4) *If K is a division ring, then its only ideals are $\{0\}$ and R.*

Lemma 12. (1) *Intersection of a family of ideals is again an ideal. (But it is NOT true for union.)*
(2) *Product of (finitely many) ideals is again an ideal.*

Proof. I leave it as an exercise. □

As in group theory, we would like to prove a statement like this

$$R_1/\ker(f) \simeq \mathrm{Im}(f).$$

So we need to say what we mean by $R_1/\ker(f)$:

Let I be an ideal of R. Then R/I is also an abelian group. Let's define the following multiplication on this group:

$$(a + I) \cdot (b + I) := (ab) + I.$$

Lemma 13. (1) *The above map is well-defined.*
(2) *$(R/I, +, \cdot)$ is a ring.*

We will prove it in the next lecture.

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

E-mail address: golsefidy@ucsd.edu