LECTURE 9.

ALIREZA SALEHI GOLSEFIDY

The starting point of lots of topics in ring theory is number theory; to be precise, the study of roots of (monic) polynomials with integer coefficients. For instance, can we talk about primes of $\mathbb{Z}[i]$? How about an arbitrary ring? Do we have unique factorization? etc.

It turns out that (for an arbitrary ring) it is better to work with ideals instead of elements.[1] So we will define a prime ideal instead of a prime element. And later (not in this course) you see that certain rings has "unique factorization" for ideals but does not have unique factorization property.

Definition 1. Let I and J be two ideals of R; then we define

$$IJ := \{\sum_i a_i b_i |\ a_i \in I,\ b_i \in J\}.$$

and

$$I + J := \{a + b |\ a \in I,\ b \in J\}.$$

Lemma 2. (1) *IJ is an ideal of R and $IJ \subseteq I \cap J$.*
(2) *$I + J$ is an ideal and moreover $\langle I \cup J\rangle = I + J$.*

Proof. 1. By the definition it is clear that IJ is closed under subtraction. Since $RI \subseteq I$ (resp. $JR \subseteq J$), we have $RIJ \subseteq IJ$ (resp. $IJR \subseteq IJ$). So IJ is an ideal.

Let $x \in IJ$. So there are $a_i \in I$ and $b_i \in J$ such that

$$x = \sum_{i=1}^{m} a_i b_i.$$

Since I (resp. J) is an ideal and $a_i \in I$ (resp. $b_i \in J$), $x = \sum_{i=1}^m a_i b_i \in I$. Hence $x \in I \cap J$.

2. Since $I+J+I+J = (I+I)+(J+J) = I+J$, $-(I+J) = (-I)+(-J) = I+J$, $R(I+J) = RI+RJ \subseteq I+J$ and $(I + J)R = IR + JR \subseteq I + J$, $I + J$ is an ideal. Since $I = I + 0 \subseteq I + J$ and $J = 0 + J \subseteq I + J$, we have $I \cup J \subseteq I + J$. Since $I + J$ is an ideal which contains $I \cup J$, we have that

$$\langle I \cup J\rangle \subseteq I + J.$$

Let $x \in I + J$; then by the definition there are $a \in I$ and $b \in J$ such that $x = a + b$. We have $a \in I \subseteq \langle I \cup J\rangle$ and $b \in J \subseteq \langle I \cup J\rangle$. Since $\langle I \cup J\rangle$ is an ideal, it is closed under addition. Thus $x = a + b \in \langle I \cup J\rangle$. Thus $I + J \subseteq \langle I \cup J\rangle$, which finished our proof. □

Definition 3. An ideal P of R is called a prime ideal if $P \neq R$ and

$$IJ \subseteq P \Rightarrow I \subseteq P \ \text{ or } \ J \subseteq P,$$

for any two ideals I and J of R.

Lemma 4. *Let R be a commutative ring. An ideal P is prime if and only if*

$$ab \in P \Rightarrow a \in P \ \text{ or } \ b \in P.$$

Date: 1/30/2012.

[1] In fact, when we are working with a PID, there is no big difference between working with elements or working with ideals. Because of this over $\mathbb{Z}$ there is no need of working with ideals.

Proof. If $ab \in P$, then $(ab) \subseteq P$. Since R is commutative, this implies that $(a)(b) = (ab) \subseteq P$. Now if P is prime, then either $(a) \subseteq P$ or $(b) \subseteq P$, and we are done.

Let $IJ \subseteq P$ and assume the contrary that $I \nsubseteq P$ and $J \nsubseteq P$. Hence there is $a \in I \setminus P$ and $b \in J \setminus P$. In particular, $ab \in IJ \subseteq P$. By our assumption, either $a \in P$ or $b \in P$, which is a contradiction. □

Example 5. *$n\mathbb{Z}$ is a prime ideal if and only if either $n = 0$ or n is prime.*

Definition 6. A proper ideal I is called a *maximal* ideal of R if

$$J \lhd R \text{ and } I \subseteq J \Rightarrow J = I \text{ or } J = R.$$

Example 7. *$n\mathbb{Z}$ is a maximal ideal if and only if n is prime.*

Lemma 8. *Let R be a unital commutative ring. Let I be an ideal in R. Then*

1. *I is a prime ideal if and only if R/I is an integral domain.*
2. *I is a maximal ideal if and only if R/I is a field.*

Proof. 1. If I is a prime ideal, then R/I is an integral domain.

$$\begin{aligned} (a+I)(b+I) = I &\Rightarrow ab \in I \\ &\Rightarrow a \in I \text{ or } b \in I \\ &\Rightarrow a + I = I \text{ or } b + I = I. \end{aligned}$$

If R/I is an integral domain, then I is a prime ideal.

$$\begin{aligned} ab \in I &\Rightarrow I = ab + I = (a+I)(b+I) \\ &\Rightarrow a + I = I \text{ or } b + I = I \\ &\Rightarrow a \in I \text{ or } b \in I. \end{aligned}$$

2. If I is a maximal ideal, then R/I is a field. Since we know that R/I is a unital commutative ring, it is enough to show that any non-zero element is a unit.

$$\begin{aligned} a + I \neq I &\Rightarrow a \notin I \\ &\Rightarrow \langle a \rangle + I = R \\ &\Rightarrow \exists\, b \in R, x \in I,\ ab + x = 1 \\ &\Rightarrow 1 + I = ab + x + I = ab + I = (a+I)(b+I) \\ &\Rightarrow a + I \in U(R/I). \end{aligned}$$

□

Corollary 9. *In a unital commutative ring any maximal ideal is a prime ideal.*

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

E-mail address: golsefidy@ucsd.edu