

Advanced Algebra II

Mar. 2, 2007 (Fri.)

assume to be commutative with identity.

We recall some basic definitions in the section.

Definition 1 *An element $a \neq 0 \in R$ is said to be a zero divisor if there is an element $b \neq 0 \in R$ such that $ab = 0$.*

A ring $R \neq 0$ and has no zero divisor is called an integral domain.

Proposition 2 *A finite integral domain is a field.*

Definition 3 *A subring $I \subset R$ is an ideal if $rx \in I$ for all $r \in R, x \in I$. It will be denoted $I \triangleleft R$.*

Proposition 4 *A subset I is an ideal if and only if for all $a, b \in I, r \in R, a + b \in I$ and $ra \in I$.*

Example 5

For $a \in R$, we have $(a) := aR$, the principal ideal generated by a .

Let $\mathfrak{N} \subset R$ be the subset of all nilpotent elements, i.e. $\mathfrak{N} := \{a \in R \mid a^n = 0, \text{ for some } n > 0\}$. Then \mathfrak{N} is an ideal, called the nilradical.

Definition 6 *An element $a \in R$ is said to be a unit if $ab = 1$ for some $b \in R$.*

Note that a is a unit if and only if $(a) = R$.

Definition 7 *An ideal \mathfrak{p} in R is prime if $\mathfrak{p} \neq R$ and if $ab \in \mathfrak{p}$ then either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.*

An ideal \mathfrak{m} in R is maximal if $\mathfrak{m} \neq R$ and if there is no ideal $I \subsetneq R$ such that $\mathfrak{m} \subsetneq I$.

It's easy to check that

Proposition 8 *$\mathfrak{p} \triangleleft R$ is prime if and only if R/\mathfrak{p} is an integral domain.*

$\mathfrak{m} \triangleleft R$ is maximal if and only if R/\mathfrak{m} is a field.

Also

Proposition 9 *$\mathfrak{P} \triangleleft R$ if and only if for any ideal $I, J \triangleleft R$, $IJ \subset \mathfrak{P}$ implies that either $I \subset \mathfrak{P}$ or $J \subset \mathfrak{P}$.*

By direct application of Zorn's Lemma, it's easy to see that in a nonzero ring, there exists a maximal ideal. We leave the detail to the readers.

A ring with exactly one maximal ideal is called a *local ring*. We have the following equivalent

conditions:

1. (R, \mathfrak{m}) is local.
2. The subset of non-units is an ideal.
3. If $\mathfrak{m} \triangleleft R$ is a maximal ideal and every element of $1 + \mathfrak{m}$ is a unit.

Proposition 10 *The nilradical is the intersection of all prime ideals.*

Exercise 11 *Let $I \triangleleft R$ be an ideal. Let $\sqrt{I} := \{x \in R \mid x^n \in I\}$. Then $\sqrt{I} = \bigcap_{\mathfrak{p}: \text{prime}, I \subset \mathfrak{p}} \mathfrak{p}$.*

Definition 12 *we define the Jacobson radical of R , denoted $\mathfrak{J}(R)$, to be the intersection of all maximal ideals.*

The Jacobson radical is clearly an ideal. It has the property that:

Proposition 13 *$x \in \mathfrak{J}$ if and only if $1 - xy$ is a unit for all $y \in R$.*

To see this, suppose that $x \in \mathfrak{J}$ and $1 - xy$ is not a unit. Then $1 - xy \in \mathfrak{m}$ for some maximal ideal \mathfrak{m} . Since $x \in \mathfrak{J} \subset \mathfrak{m}$, we have $1 \in \mathfrak{m}$, a contradiction.

Conversely, if $x \notin \mathfrak{J}$, then $x \notin \mathfrak{m}$ for some maximal ideal \mathfrak{m} . Then $\mathfrak{m} + (x) = R$. So we have $1 = xy + u$ for some $u \in \mathfrak{m}$, and hence $1 - xy = u$ is not a unit.

Theorem 14 (Chinese remainder theorem)

Let I_1, \dots, I_n be ideals of R such that $I_i + I_j = R$ for all $i \neq j$. Given elements $x_1, \dots, x_n \in R$, there exists $x \in R$ such that $x \equiv x_i \pmod{I_i}$ for all i .

The proof is left to the readers as an exercise.

Corollary 15 *Let I_1, \dots, I_n be ideals of R such that $I_i + I_j = R$ for all $i \neq j$. Let $f : R \rightarrow \prod_{i=1}^n R/I_i$. Then f is surjective with kernel $\cap I_i$.*

Factorization

Definition 16 A non-zero element $a \in R$ is said to be divide $b \in R$, denoted $a|b$ if there is $c \in R$ such that $ac = b$.

Elements $a, b \in R$ are said to be associate, denoted $a \sim b$, if $a|b$ and $b|a$.

The following properties are immediate.

1. $a|b$ if and only if $(a) \supset (b)$.
2. $a \sim b$ if and only if $(a) = (b)$.
3. a is a unit if and only if $(a) = R$.

Definition 17 A non-zero non-unit $c \in R$ is said to be **irreducible** if $c = ab$ then either a or b is unit.

A non-zero non-unit $p \in R$ is said to be **prime** if $p|ab$ then $p|a$ or $p|b$.

Then we have the following:

Proposition 18 *Let p, c are non-zero non-unit elements in R .*

1. *p is prime if and only if (p) is prime.*
2. *c is irreducible if and only if (c) is maximal among all proper principal ideals.*
3. *Prime element is irreducible.*
4. *If R is a PID, then p is prime if and only if p is irreducible.*
5. *If $a = bu$ with u a unit, then $a \sim b$.*
6. *If R an integral domain, then $a \sim b$ implies $a = bu$ for some unit u .*

Definition 19 *An integral domain is called a unique factorization domain, UFD for short, if every non-zero non-unit element can be factored into products of irreducible elements. And the factorization is unique up to units.*

Definition 20 *A ring R is said to be an Euclidean ring if there is a function $\varphi : R - \{0\} \rightarrow \mathbb{N}$*

such that:

1. if $a, b \neq 0 \in R$ and $ab \neq 0$, then $\varphi(a) \leq \varphi(ab)$.
2. if $a, b \neq 0 \in R$, then there exist $q, r \in R$ such that $a = qb + r$ with either $r = 0$ or $r \neq 0$ and $\varphi(r) < \varphi(b)$.

Lemma 21 Let R be a PID, then its ideals satisfies Ascending chain condition, i.e. for an ascending chain of ideals

$$I_1 \subset I_2 \dots$$

there is n such that $I_n = I_{n+1} = \dots$

Theorem 22 *Every Euclidean domain, ED for short, is a PID. Every PID is a UFD.*

Localization

We need to recall some basic notion of localization.

Definition 23 *A subset $S \subset R$ is said to be a multiplicative set if*

1. $1 \in S$,
2. *if $a, b \in S$, then $ab \in S$.*

Given a multiplicative set, then one can construct a localized ring $S^{-1}R$ which I suppose the readers have known this. In order to be self-contained, I recall the construction:

In $R \times S$, we define an equivalent relation that $(r, s) \sim (r', s')$ if $(rs' - r's)t = 0$ for some $t \in S$. Let $\frac{r}{s}$ denote the equivalent class of (r, s) . One can define addition and multiplication naturally. The set of all equivalent classes, denoted

$S^{-1}R$, is thus a ring. There is a natural ring homomorphism $\iota : R \rightarrow S^{-1}R$ by $\iota(r) = \frac{r}{1}$.

Remark 24

1. If $0 \in S$, then $S^{-1}R = 0$. We thus assume that $0 \notin S$.
2. If R is a domain, then ι is injective. And in fact, $S^{-1}R \hookrightarrow F$ naturally, where F is the quotient field of R .
3. Let $J \triangleleft S^{-1}R$. We will use $J \cap R$ to denote the ideal $\iota^{-1}(J)$. (If R is a domain, then $J \cap R = \iota^{-1}(J)$ by identifying R as a subring of $S^{-1}R$).

I would like to recall the most important example and explain their geometrical meaning, which, I think, justify the notion of localization.

Example 25 Let $f \neq 0 \in k[x_1, \dots, x_n]$ and let $S = \{1, f, f^2, \dots\}$. The localization $S^{-1}k[x_1, \dots, x_n]$ is usually denoted $k[x_1, \dots, x_n]_f$. This ring can

be regarded as "regular functions" on the open set $U_f := \mathbb{A}_k^n - \mathcal{V}(f)$. One notices that U_f is of course the maximal open subset that the ring $k[x_1, \dots, x_n]_f$ gives well-defined functions.

Example 26 Let $x = (a_1, \dots, a_n) \in \mathbb{A}_k^n$ and $\mathfrak{m}_x = (x_1 - a_1, \dots, x_n - a_n)$ be its maximal ideal. Take $S = k[x_1, \dots, x_n] - \mathfrak{m}_x$, then the localization is denoted $k[x_1, \dots, x_n]_{\mathfrak{m}_x}$. It is the ring of regular functions "near x ".

Recall that for a R -module M , one can also define $S^{-1}M$ which is naturally an $S^{-1}R$ -module. And we have:

Proposition 27

1. If $I \triangleleft R$, then $S^{-1}I \triangleleft S^{-1}R$. Moreover, every ideal $J \triangleleft S^{-1}R$ is of the form $S^{-1}I$ for some $I \triangleleft R$.

2. For $J \triangleleft S^{-1}R$, then $S^{-1}(J \cap R) = J$.
3. $S^{-1}I = S^{-1}R$ if and only if $I \cap S \neq \emptyset$.
4. There is a one-to-one correspondence between $\{\mathfrak{p} \in \text{Spec}(R) \mid \mathfrak{p} \cap S = \emptyset\}$ and $\{\mathfrak{q} \in \text{Spec}(S^{-1}R)\}$.
5. In particular, the prime ideals of the local ring $R_{\mathfrak{p}}$ are in one-to-one correspondence with the prime ideals of R contained in \mathfrak{p} .

But for $I \triangleleft R$, then $S^{-1}I \cap R \supset I$ only. Indeed, if $x \in I \triangleleft R$. Then $x = \frac{xs}{x} \in S^{-1}I \cap R$. Conversely, for $x \in S^{-1}I \cap R$, then $\frac{x}{1} = \frac{y}{t}$ for some $y \in I$. Thus $(y - xt)s = 0$ for some $s, t \in S$. We can not get $y \in I$ in general. However, this is the case if I is prime and $S \cap I = \emptyset$. Thus we have

Proposition 28 *If $\mathfrak{p} \triangleleft R$ is a prime ideal and $S \cap \mathfrak{p} = \emptyset$. Then $S^{-1}\mathfrak{p} \cap R = \mathfrak{p}$.*

Example 29 *Let $\mathfrak{p} \in \text{Spec}(R)$, then $R_{\mathfrak{p}}$ is a local ring with the unique maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$. To see that, if there is a maximal ideal \mathfrak{m} . By the correspondence, $\mathfrak{m} = \mathfrak{q}R_{\mathfrak{p}}$ for some $\mathfrak{q} \subset \mathfrak{p}$. Thus $\mathfrak{m} \subset \mathfrak{p}R_{\mathfrak{p}}$ and thus must be equal.*

A ring with a unique maximal ideal is called a local ring. Thus $R_{\mathfrak{p}}$ is a local ring.

Proposition 30 *The operation S^{-1} on ideals commutes with formation of finite sums, product, intersection and radicals.*

Another important feature is that

Proposition 31 *The operation S^{-1} is exact. That is, if*

$$M' \xrightarrow{f} M \xrightarrow{g} M''$$

is an exact sequence of R -module, then

$$S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M''$$

is exact as $S^{-1}R$ -module.

Corollary 32 *The operation S^{-1} commutes with passing to quotients by ideals. That is, let $I \triangleleft R$ be an ideal and \bar{S} the image of S in $\bar{R} := R/I$. Then $S^{-1}R/S^{-1}I \cong \bar{S}^{-1}\bar{R}$.*