Introduction to Rings and Modules

Lecture 10, Wednesday May 17 2023
Ari Feiglin

Definition 10.0.1:

If R is a commutative ring and $S \subseteq R$, S is called a **multiplicative set** if $0 \notin S$, $1 \in S$, and S is closed under multiplication.

Note that a multiplicative set S cannot contain zero divisors, since then their product, zero, would be in S.

Example 10.0.2:

(1) $S = \{1\}$ is always multiplicative, if R is not trivial.

(2) If R is an integral domain, $S = R \setminus \{0\}$ is a multiplicative set.

(3) If $P \trianglelefteq R$ is prime, $R \setminus P$ is also multiplicative. And if $\{P_\lambda\}_{\lambda \in \Lambda}$ is a set of prime ideals, $R \setminus \bigcup_\Lambda P_\lambda$ is a multiplicative set.

Given a commutative ring R and a multiplicative set S, we define an equivalence relation on $R \times S$ by $(r_1, s_1) \sim (r_2, s_2)$ if there exists a $t \in S$ such that $t(r_1 s_2 - r_2 s_1) = 0$. If R is an integral domain, this is equivalent to $r_1 s_2 = r_2 s_1$.
This is obviously reflexive and symmetric, we will show that it is also transitive. Suppose $(r_1, s_1) \sim (r_2, s_2)$ and $(r_2, s_2) \sim (r_3, s_3)$. Suppose $t_1(r_1 s_2 - r_2 s_2) = 0$ and $t_2(r_2 s_3 - r_3 s_2) = 0$. Notice then that since the ring is commutative

$$0 = (s_3 t_2) t_1 (r_1 s_2 - r_2 s_2) + (s_2 t_1) t_2 (r_2 s_3 - r_3 s_2) = t_1 t_2 (r_2 s_2 s_3 - r_2 s_2 s_3 + r_2 s_2 s_3 - r_3 s_2 s_2) = t_1 t_2 s_2 (r_2 s_3 - r_3 s_2)$$

and since S is closed under multiplication, $t_1 t_2 s_2 \in S$, and so we have that $(r_2, s_2) \sim (r_3, s_3)$ as required.

Definition 10.0.3:

If R is a commutative ring and $S \subseteq R$ is a multiplicative set, we define $S^{-1}R$ to be the partition of R by the equivalence relation defined above. We endow it with a ring structure by defining:

$$\big[(r_1, s_1)\big] + \big[(r_2, s_2)\big] = \big[(r_1 s_2 + r_2 s_1, s_1 s_2)\big]$$

(this should be reminiscient of fraction addition), and

$$\big[(r_1, s_1)\big] \cdot \big[(r_2, s_2)\big] = \big[(r_1 r_2, s_1 s_2)\big]$$

We denote $\big[(r, s)\big]$, the equivalence class of (r, s), by $\frac{r}{s}$ (there are many ways to write the same fraction). And $S^{-1}R$ is called the **localization** of R by S.

These operations are well-defined, and this is indeed a (commutative) ring. Its additive identity is $\frac{0}{1} = \big[(0, 1)\big]$ since $\frac{0}{1} + \frac{a}{b} = \frac{0b + a1}{1b} = \frac{a}{b}$, and its multiplicative identity is $\frac{1}{1} = \big[(1, 1)\big]$ since $\frac{1}{1} \cdot \frac{a}{b} = \frac{a}{b}$.
Notice that $\frac{s}{s} = \frac{1}{1}$, since $s - s = 0$ so taking $t = 1$ satisfies the relation. And $\frac{0}{s} = \frac{0}{0}$ since $0 \cdot 0 - 0 \cdot s = 0$.

Proposition 10.0.4:

Let R be an integral domain, and $S = R \setminus \{0\}$. Then $S^{-1}R$ is a field.

Proof:

Let $\frac{0}{1} \neq \frac{r}{s} \in S^{-1}R$, this is equivalent to $0 \cdot s \neq 1 \cdot r$, so $0 \neq r$. Then $r \in S$, and so $\frac{s}{r}$ exists and

$$\frac{r}{s} \cdot \frac{s}{r} = \frac{rs}{rs} = \frac{1}{1}$$

so it is the inverse of $\frac{r}{s}$. ∎

Example 10.0.5:

(1) If $R = \mathbb{Z}$ and $S = \mathbb{Z} \setminus \{0\}$ then $S^{-1}R = \mathbb{Q}$.

(2) And if $R = \mathbb{Z}$ and $S = \{2^n \mid n \geq 0\}$ then $S^{-1}R = \left\{x \in \mathbb{Q} \;\middle|\; x = \frac{a}{2^n}, a \in \mathbb{Z}, n \geq 0\right\}$.

Proposition 10.0.6:

Let R be an integral domain, and $p \in R$ is prime. Then p is irreducible.

Proof:

Suppose $p = ab$, then $ab \in (p)$ which is prime, and so $a \in (p)$ or $b \in (p)$. Without loss of generality, suppose $a \in (p)$, so $a = px$. Then $p = pxb$ and so $p(1 - xb) = 0$, and since R is an integral domain, $1 = xb$ and so b is invertible. Thus p is irreducible. ■

Example 10.0.7:

Even if R is an integral domain, irreducible numbers aren't necessarily prime. Take $R = \mathbb{Z}[\sqrt{-5}]$, and $2 \in R$. Again we introduce the norm $N(a + b\sqrt{-5}) = a^2 + 5b^2$ which is multiplicative. Then 2 is irreducible since if $2 = xy$ then $4 = N(x)N(y)$, but $N(x) \neq 2$ since this has no solutions, so $N(x) = 1$ or $N(x) = 4$. If $N(x) = 1$ then x is invertible, and if $N(x) = 4$ then $N(y) = 1$ so y is irreducible.
But let $\alpha = (1 + \sqrt{-5})$ and $\beta = (1 - \sqrt{-5})$ then $\alpha\beta = 6 = 2 \cdot 3$. So $2|\alpha\beta$, but $N(\alpha) = 6$ and $N(\beta) = 6$ and since $N(2) = 4$, which does not divide 6, 2 does not divide α or β. So 2 is irreducible, but not prime.

Proposition 10.0.8:

Let R be a UFD, then an element is prime if and only if it is irreducible.

Proof:

If p is prime, it is irreducible. If p is irreducible, suppose $p|ab$, then $ab = px$. By factorizing x, we can factorize $ab = px$ as

$$ab = px = p(q_1 \cdots q_n)$$

Since p is irreducible, And a and b can be factorized as

$$a = q_1' \cdots q_r', \qquad b = q_1'' \cdots q_s''$$

then

$$ab = q_1' \cdots q_r' \cdot q_1'' \cdots q_s''$$

And since factorization is unique, p is friends with some q_i' or q_i''. Without loss of generality $q_i' = pu$ where u is invertible. But then

$$a = q_1' \cdots up \cdots q_n' = p(q_1' \cdots u \cdots q_n'$$

and so $p|a$, so p is prime. ■

Definition 10.0.9:

If R is a ring, we denote the set of all invertible elements in R by $R^\times$.

Proposition 10.0.10:

If R is an integral domain, then

(1) $R[x]$ is also an integral domain.

(2) $R[x]^\times = R^\times$.

Proof:

(1) Suppose $P, Q \in R[x]$ and

$$P = \sum_{k=0}^{n} a_n x^n, \qquad Q = \sum_{k=0}^{m} b_m x^m$$

where $a_n, b_m \neq 0$. Then

$$PQ = \sum_{k=0}^{n+m} x^k \sum_{i=0}^{k} a_i b_{k-i} = a_n b_m x^{n+m} + \cdots$$

Therefore $\deg(PQ) = \deg P + \deg Q$. So if $PQ = 0$ then $0 = \deg 0 = \deg(PQ) = \deg P + \deg Q$. Thus $\deg P = \deg Q = 0$ and so P and Q are constants, but $PQ = 0$ and R is an integral domain, so $p = 0$ or $Q = 0$.

(2) It is obvious that $R^\times \subseteq R[x]^\times$. Now suppose that $P \in R[x]^\times$, then $PP^{-1} = 1$ is constant, so $0 = \deg(PP^{-1}) = \deg P + \deg P^{-1}$ and so $\deg P = \deg P^{-1} = 0$, meaning $P, P^{-1} \in R$. So $P \in R^\times$. ■

Lemma 10.0.11:

If $\varphi\colon R \longrightarrow S$ is a ring homomorphism, this defines a ring homomorphism $\psi\colon R[x] \longrightarrow S[x]$ by

$$\psi\left(\sum_{k=0}^{n} a_k x^k\right) = \sum_{k=0}^{n} \varphi(a_k) x^k$$

The kernel of φ is given by $(\operatorname{Ker}\varphi)[x]$. And whose image is $\varphi(R)[x]$.

Proof:

This is additive:

$$\psi\left(\sum_{k=0}^{n} a_k x^k + \sum_{k=0}^{n} b_k x^k\right) = \sum_{k=0}^{n} \varphi(a_k + b_k) x^k = \sum_{k=0}^{n} \varphi(a_k) x^k + \sum_{k=0}^{n} \varphi(b_k) x^k$$

as required. And it is multiplicative:

$$\psi\left(\sum_{k=0}^{n} a_k x^k \cdot \sum_{k=0}^{m} b_k x^k\right) = \sum_{k=0}^{n+m} x^k \sum_{i=0}^{k} \varphi(a_i b_{k-i}) = \sum_{k=0}^{n} \varphi(a_k) x^k \cdot \sum_{k=0}^{m} \varphi(b_k) x^k$$

as required.
And $\sum_0^n a_k x^k \in \operatorname{Ker}\psi$ if and only if for every k, $\varphi(a_k) = 0$. This is if and only if $a_k \in \operatorname{Ker}\varphi$ for every k, meaning the polynomial is in $(\operatorname{Ker}\varphi)[x]$. And it is simple to see that $\psi(R[x]) = \varphi(R)[x]$. ■

Proposition 10.0.12:

Let R be a ring and $I \subseteq R$ be a left/right/bidirectional ideal. Then let $I[x] = \{a_n x^n + \cdots + x_0 \mid a_i \in I\}$ is a left/right/bidirectional ideal of $R[x]$. And if I is a bidirectional ideal then

$$R[x] \big/ I[x] \cong R \big/ I\, [x]$$

Proof:

We will prove this for right ideals. It is obvious that I is closed under addition and additive inverses, and contains 0 (these are a direct result of I being so). Then if $P \in I[x]$ and $Q \in R[x]$, suppose

$$P = \sum_{k=0}^{n} a_k x^k, \qquad Q = \sum_{k=0}^{m} b_k x^k$$

then

$$PQ = \sum_{k=0}^{n+m} x^k \sum_{i=0}^{k} a_i b_{k-i}$$

since I is a right ideal, for every i and k, $a_i b_{k-i} \in I$, and so the sum $\sum_{i=0}^{k} a_i b_{k-i} \in I$. Therefore $PQ \in I[x]$, and so $I[x]$ is a right ideal as required.
Note that if I is a bidrectional ideal, it is both a left and right ideal, and so $I[x]$ is both a left and right ideal, so $I[x]$ is a bidrectional ideal. We take the cannonical homomorphism

$$\varphi \colon R \longrightarrow {}^{R}\!/_{I}, r \mapsto r + I$$

The kernel of φ is I, and it is surjective. By the lemma above, this defines a homomorphism

$$\psi \colon R[x] \longrightarrow \left({}^{R}\!/_{I}\right)[x]$$

whose kernel is $(\operatorname{Ker} \varphi)[x] = I[x]$, and image is $\varphi(R)[x] = \left({}^{R}\!/_{I}\right)[x]$ as required. By the first isomorphism theorem, we have

$${}^{R[x]}\!/_{I[x]} \cong \left({}^{R}\!/_{I}\right)[x]$$

as required. ■