Introduction to Rings and Modules

Lecture 5, Monday April 24 2023
Ari Feiglin

Example 5.0.1:

Suppose that R is commutative and $I = (a)$ and $J = (b)$ are two ideals, then $IJ = (ab)$. This is because $a \in I$ and $b \in J$ so $ab \in IJ$ and thus $(ab) \subseteq IJ$ (since $(ab) = abR$). And every element in IJ is of the form $\sum_{k=1}^{n} i_k j_k$ where $i_k \in I$ and $j_k \in J$ so $i_k = ar_n$ and $j_k = bs_n$. Thus the element is

$$\sum_{k=1}^{n} ar_n bs_n = ab \sum_{k=1}^{n} r_n s_n \in abR = (ab)$$

so $IJ \subseteq (ab)$ and thus $IJ = (ab)$ as required.

Notice that if $R = \mathbb{R}[x]$ and $I = (x-1)$ and $J = (x+1)$ then by above $IJ = (x^2-1)$ so by the chinese remainder theorem:

$$\mathbb{R}[x] \big/ (x^2-1) \cong \mathbb{R}[x] \big/ (x-1) \times \mathbb{R}[x] \big/ (x+1) \cong \mathbb{R} \times \mathbb{R}$$

where the last equality is true since we showed that $\mathbb{R}[x] / (x-a) \cong \mathbb{R}$. So notice that while $\mathbb{R}[x] \big/ (x^2+1) \cong \mathbb{C}$ is a field, $\mathbb{R}[x] \big/ (x^2-1) \cong \mathbb{R}^2$ is not a field since there are zero divisors: $(1,0) \cdot (0,1) = 0$.

The chinese remainder theorem has its limits, specifically when the ideals are not comaximal. For example $\mathbb{R}[x] \big/ (x^2)$ since $(x^2) = (x)(x)$ and (x) is not comaximal with itself (in general groups G satisfy $G \cdot G = G$, and this holds with ideals $I + I = I$). But we can take $y = x + (x^2) \in \mathbb{R}[x] \big/ (x^2)$ and so $y^2 = x^2 + (x^2) = (x^2) = 0_R$ (y is nilpotent). Notice that $\mathbb{R}[x] \big/ (x^2-1)$ has no such non-trivial element since $(x,y)^2 = 0 \implies (x,y) = 0$, and therefore these two rings cannot be isomorphic.

So these three rings are all non-isomorphic.

Proposition 5.0.2:

Suppose $f\colon R \longrightarrow S$ is a ring homomorphism, then

(1) If $R' \subseteq R$ is a subring or subrng of R then $f(R')$ is a subring or subrng of S.

(2) If $J \subseteq S$ is a (left, right, or bidirectional) ideal of S then $f^{-1}(J)$ is a (left, right, or bidirectional) ideal of R.

(3) If $I \subseteq R$ is a (left, right, or bidirectional) ideal of R then $f(I)$ is a (left, right, or bidirectional) ideal of $f(R)$.

Proof:

Notice that in all cases, $f(X)$ or $f^{-1}(X)$ are abelian groups as the image or preimage of an abelian group. So for these proofs all we need to show is the multiplicative nature of whatever we're investigating.

(1) Suppose $f(x), f(y) \in f(R')$ then $f(x)f(y) = f(xy) \in R'$ as required. And if f is a ring homomorphism and R' is a subring then $1_R \in R'$ so $f(1_R) = 1_S \in f(R')$ as required.

(2) We will assume that J is a right ideal, the proofs for the other cases are identical. Suppose $x \in f^{-1}(J)$ then we must show for any $r \in R$, $xr \in f^{-1}(J)$. This is if and only if $f(xr) = f(x)f(r)$, since $f(x) \in J$ and $f(r) \in S$, $f(x)f(r) \in J$ so $f(xr) \in J$ and so $xr \in f^{-1}(J)$ as required.

(3) Again we suppose I is a right ideal. Suppose $f(x) \in f(I)$ and $f(r) \in f(R)$ then $f(x)f(r) = f(xr)$, and since $xr \in I$, $f(x)f(r) \in f(I)$ as required. $\blacksquare$

Notice that since $\{0\}$ is an ideal of S, we get that $\operatorname{Ker} f = f^{-1}\{0\} \trianglelefteq R$ from the above proposition.

Note:

If $\mathbb{F}$ is a field and $I \trianglelefteq \mathbb{F}$ is an ideal, if $I \neq (0)$ then there exists an $a \in I$ such that $a \neq 0$ so $a^{-1} \cdot a = 1 \in I$ and so $I = \mathbb{F}$. Thus the ideals of fields are all trivial.

Theorem 5.0.3:

Suppose R is a ring and $I \trianglelefteq R$ is a bidirectional ideal, then there is a pairing between right/left/bidirectional ideals of ${}^{R}\!/_{I}$ and right/left/bidirectional ideals of R which contain I.

Definition 5.0.4:

Suppose R is a commutative ring. An ideal $I \trianglelefteq R$ is **prime** if I is not trivial and for every $a, b \in R$ if $ab \in I$ then either $a \in I$ or $b \in I$.

Example 5.0.5:

Notice then that if p is prime, then $p\mathbb{Z}$ is a prime ideal. This is because if $nm \in p\mathbb{Z}$ then p divides nm and therefore divides n or m and so one is in $p\mathbb{Z}$.
And if n is not prime then suppose p is a prime which divides n, then $p \cdot \frac{n}{p} \in n\mathbb{Z}$ but neither p nor $\frac{n}{p}$ are in $n\mathbb{Z}$, so $n\mathbb{Z}$ is not prime. So the only prime ideals of $\mathbb{Z}$ are $p\mathbb{Z}$.

Proposition 5.0.6:

Let R be a commutative ring, and $I \trianglelefteq R$. The following are equivalent:

(1) I is a prime ideal.

(2) For any $J, J' \trianglelefteq R$, if $JJ' \subseteq I$ then $J \subseteq I$ or $J' \subseteq I$.

(3) ${}^{R}\!/_{I}$ is an integral domain.

Proof:

We show the first equivalence. Suppose that there is an $a \in J$ which isn't in I and a $b \in J'$ which isn't in I. But $ab \in JJ' \subseteq I$ and since I is prime, $a \in I$ or $b \in I$.
Now we show the second equivalence. Suppose that

$$(r + I)(r' + I) = I \implies rr' + I = I$$

then $rr' \in I$ so one must be in I, so one of $r + I$ or $r' + I$ is 0, so ${}^{R}\!/_{I}$ is an integral domain.
We show that the third implies the first. Suppose $ab \in I$ then $(a + I)(b + I) = ab + I = 0_{{}^{R}\!/_{I}}$. But since ${}^{R}\!/_{I}$ is an integral domain, $a + I$ or $b + I$ must be 0 so either $a \in I$ or $b \in I$ as required. $\blacksquare$