Introduction to Rings and Modules

Lecture 2, Monday March 20 2023
Ari Feiglin

2.1 Subrings

Definition 2.1.1:

Let R be a ring, and $\varnothing \neq S \subseteq R$. Then S is a **subring** of R if it satisfies the following:

(1) $(S, +)$ is a subgroup of $(R, +)$ (equivalently it is closed under subtraction, if $a, b \in S$ then $a - b \in S$).

(2) S is closed under multiplication: if $a, b \in S$ then $a \cdot b \in S$.

(3) $1_R \in S$.

Equivalent to the last two conditions is that $(S, \cdot)$ is a submonoid of $(R, \cdot)$.
If we remove the third condition, then S is a **subrng** (if $(S, +)$ is a subgroup of $(R, +)$ and S is closed under multiplication, then S is a subrng).

Note that $\varnothing S \subseteq R$ is a subrng of R if and only if S is a rng.

Example 2.1.2:

Let $R = M_2(\mathbb{Z})$ be our ring and

$$S = \left\{ \begin{pmatrix} a & a \\ 0 & 0 \end{pmatrix} \;\middle|\; a \in \mathbb{Z} \right\}$$

be a subset of R. Then S is not a subring of R's since the identity is not in S, but S *is* a ring under the same operations as R:

(1) It is closed under addition and inverses, so $(S, +)$ is a group (it is a subgroup of $(R, +)$).

(2) It is closed under multiplication, and $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ is its identity, so $(S, \cdot)$ is a monoid.

And so S is indeed a ring, but not a subring (and therefore S is a subrng).
So it is not sufficient to show that $\varnothing \neq S \subseteq R$ is a ring, we must show it is a ring where the identity is 1_R. This is true since then $(S, +)$ is a group and since $S \subseteq R$ it is a subgroup of $(R, +)$. And it is necessarily closed under multiplication since it is a ring, and $1_R \in S$ by assumption

Example 2.1.3:

Let $R = \mathbb{Z}$, then every subring of R must, by definition, contain 1. But since $(S, +)$ is a group, $\mathbb{Z} = \langle 1 \rangle \subseteq S \implies S = \mathbb{Z}$. So $\mathbb{Z}$ has no non-trivial subrings.

Example 2.1.4:

Let $\mathbb{F}$ be a field and $R = \mathbb{F}[x]$. Then let $a \in \mathbb{F}$ and $S = \{P \in R \mid P(a) = 0_{\mathbb{F}}\}$. S is closed under subtraction since if $P(a) = Q(a) = 0$ then $\big(P - Q\big)(a) = P(a) - Q(a) = 0$. And it is closed under multiplication since $\big(PQ\big)(a) = P(a)Q(a) = 0$ since $\mathbb{F}$ is a field. But $1 \notin S$ so S is a subrng but not a subring.

Example 2.1.5:

If $\{R_\lambda\}_{\lambda \in \Lambda}$ are rings, then their **product ring**: $R = \prod_{\lambda \in \Lambda} R_\lambda$ is also a ring. The operations are

$$\big(f + g\big)(\lambda) = f(\lambda) + g(\lambda) \in R_\lambda, \qquad \big(f \cdot g\big)(\lambda) = f(\lambda) \cdot g(\lambda) \in R_\lambda$$

The additive identity is $0(\lambda) = 0_{R_\lambda}$ and the multiplicative identity is $1(\lambda) = 1_{R_\lambda}$. The proof that this is indeed a ring

is trivial.
And if S_λ is a subring of R_λ then $S=\prod_{\lambda\in\Lambda}S_\lambda$ is a subring of R (again, this is trivial).

Example 2.1.6:

If R is a ring and $y\in R$ then the **center** of y is

$$C_R(y)=\{a\in R \mid ay=ya\}$$

the center of y is a subring of R:

(1) If $a,b\in C_R(y)$ we must show that $(a+b)y=y(a+b)$, and we know $(a+b)y=ay+by=ya+yb=y(a+b)$ as required. And if $a\in C_R(y)$ then $(-a)y=-(ay)$ since $(-a)y+ay=(-a+a)y=0y=0$, and so $(-a)y=-(ay)=-(ya)=y(-a)$ (the last equality is similarly trivial). So $C_R(y)$ is a group under addition.

(2) If $a,b\in C_R(y)$ then $(ab)y=a(by)=a(yb)=(ay)b=(ya)b=y(ab)$ so $ab\in C_R(y)$.

(3) And $1\in C_R(y)$ trivially.

Proposition 2.1.7:

If $\{S_\lambda\}_{\lambda\in\Lambda}$ are subrings of R, then $S=\bigcap_{\lambda\in\Lambda}S_\lambda$ is also a subring of R.

Proof:

We know that $1_R\in S$ because it is in every S_λ. Suppose $a,b\in S$ then $a,b\in S_\lambda$ for every $\lambda\in\Lambda$ so $a-b\in S_\lambda$ for every $\lambda\in\Lambda$ and so $a-b\in S$, so $(S,+)$ is a subgroup of $(R,+)$. And if $a,b\in S$ then $a,b\in S_\lambda$ and so $ab\in S_\lambda$ for every $\lambda\in\Lambda$ and so $ab\in S$. So S is indeed a subring of R.

■

Definition 2.1.8:

Suppose R is a ring, then we define its **center** to be:

$$\mathrm{Z}(R)=\{a\in R \mid \forall b\in R: ab=ba\}$$

It is trivial to see that:

$$\mathrm{Z}(R)=\bigcap_{a\in R}C_R(a)$$

and so $\mathrm{Z}(R)$ is a subring of R's.

2.2 Ring Homomorphisms

Definition 2.2.1:

Suppose R and S are two rings, then a function $f\colon R\longrightarrow S$ is a **ring homomorphism** if it satisfies:

(1) For every $a,b\in R$, $f(a+_R b)=f(a)+_S f(b)$ (f is a group homomorphism between $(R,+_R)$ and $(S,+_S)$).

(2) For every $a,b\in R$, $f(a\cdot_R b)=f(a)\cdot_S f(b)$.

(3) $f(1_R)=1_S$.

If R and S are rngs, and $f\colon R\longrightarrow S$ satisfies the first two properties above, it is a **rng homomorphism**.

Example 2.2.2:

If $S\subseteq R$ is a subring of R's, then $f\colon S\longrightarrow R$ defined by $f(s)=s$ is called the **inclusion monomorphism**.

Example 2.2.3:

If R is a ring, then if $f\colon \mathbb{Z} \longrightarrow R$ is a ring homomorphism, $f(1) = 1_R$ and this defines the image of every $n \in \mathbb{Z}$: $f(n) = 1_R + \cdots + 1_R = [n]_R$. This homomorphism is also well-defined, the first axiom is trivial. And the second axioms follows from $f(n \cdot m) = [nm]_R = [n]_R[m]_R = f(n) \cdot f(m)$. And by definition $f(1) = 1_R$.
So there exists exactly one ring homomorphism from $\mathbb{Z}$ to R for every ring R.

Example 2.2.4:

Let R be a ring, and $b \in R$. We define the **evaluation** of b is $\mathrm{ev}_b\colon R[x] \longrightarrow R$ defined by $\mathrm{ev}_b(P) = P(b)$. This obviously satisfies the first axiom. Now suppose

$$P = \sum_{i=0}^{n} a_i x^i, \qquad Q = \sum_{i=0}^{n} c_i x^i$$

then

$$PQ = \sum_{k=0}^{2n} \sum_{i+j=k} a_i c_j x^k$$

And so we have that:

$$\mathrm{ev}_b(PQ) = \sum_{k=0}^{2n} \Bigg(\sum_{i+j=k} a_i c_j \Bigg) b^k$$

If $b \in \mathrm{Z}(R)$ then

$$= \sum_{k=0}^{2n} a_i b^i c_j b^j = \left(\sum_{i=0}^{n} a_i b^i \right) \cdot \left(\sum_{j=0}^{n} c_j b^j \right) = P(b) \cdot Q(b) = \mathrm{ev}_b(P) \cdot \mathrm{ev}_b(Q)$$

And the third axiom is trivial since $1_{R[x]}(b) = 1_R$.
So if $b \in \mathrm{Z}(R)$ then ev_b is a ring homomorphism.

Example 2.2.5:

Suppose $f\colon R \longrightarrow S$ is a ring homomorphism, then we define $F\colon M_n(R) \longrightarrow M_n(S)$ by $F\big((a_{ij})\big) = \big(f(a_{ij})\big)$, ie we take the image of each element in the matrix. Obviously

$$F\big((a_{ij}) + (b_{ij})\big) = \big(f(a_{ij} + b_{ij})\big) = \big(f(a_{ij}) + f(b_{ij})\big) = \big(f(a_{ij})\big) + \big(f(b_{ij})\big) = F\big((a_{ij})\big) + F\big((b_{ij})\big)$$

And:

$$F\big((a_{ij}) \cdot (b_{ij})\big) = F\left(\left(\sum_{k=1}^{n} a_{ik} b_{kj} \right) \right) = \left(f\left(\sum_{k=1}^{n} a_{ik} b_{kj} \right) \right) = \left(\sum_{k=1}^{n} f(a_{ik}) f(b_{kj}) \right) = \big(f(a_{ij})\big) \cdot \big(f(b_{ij})\big) = F\big(a_{ij}\big) \cdot F\big((b_{ij})\big)$$

And $F(I_R) = I_S$ is obvious.