MATH 8510, Abstract Algebra I
Fall 2016
Exercises 13-1
Collbrators: Dazhou Zhu, Xiaoyuan Liu
Name: Shuai Wei

Exercise 1. Let R be a commutative ring with identity.

(a) Let $A, B \subseteq R$ and set $I = (A)R$ and $J = (B)R$. Prove that $I + J$ is generated by $A \cup B$.

Proof. (1) If $A = B = \emptyset$, we have $A \cup B = \emptyset$ and $I = J = \{0\}$. Then

$$I + J = \{0\} = (\emptyset)R = (A \cup B)R.$$

So $I + J$ is generated by $A \cup B$.

(2) If $A = \emptyset$ and $B \neq \emptyset$, we have $A \cup B = B$ and

$$I + J = (\emptyset)R + (B)R = \{0\} + (B)R = (B)R = (A \cup B)R.$$

So $I + J$ is generated by $A \cup B$.

(3) Assume $A \neq \emptyset$ and $b \neq \emptyset$.
Since $(A)R = I \leq R$ and $(B)R = J \leq R$,
we have

$$I + J \leq R.$$

Since $A \subseteq A \cup B$,

$$I = (A)R \subseteq (A \cup B)R.$$

Similarly,

$$J \subseteq (A \cup B)R.$$

By the definition of $I + J$, we have

$$I + J \subseteq (A \cup B)R. \tag{1}$$

Since R is CRW1,

$$(A \cup B)R = \{\sum_{i}^{\text{finite}} c_i r_i \mid c_i \in A \cup B, r_i \in R\}.$$

Let $x \in (A \cup B)R$, then $\exists\ N \in \mathbb{N}$ and $c_i \in A \cup B$ and $r_i \in R$ for $i = 1, 2, \cdots, N$ such that

$$x = \sum_{i}^{N} c_i r_i.$$

Without loss of generality, assume $\exists\ c_i \in A$ for some integer i between 1 and N.

Rearrange $\{c_i r_i, i = 1, \cdots, N\}$ such that $c_i \in A$ for $i = 1, \cdots, M$ and $c_i \in B$ for $i = M+1, \cdots, N$, where $M \in \mathbb{N}$ and $1 \leq M \leq N$.
Then

$$\begin{aligned} x &= \sum_{i}^{M} c_i r_i + \sum_{i=M+1}^{N} c_i r_i \\ &\in (A)R + (B)R \\ &= I + J. \end{aligned}$$

So

$$(A \cup B)R \subseteq I + J. \tag{2}$$

Thus, by (1) and (2), we have

$$I + J = (A \cup B)R.$$

Therefore, $I + J$ is generated by $A \cup B$.

□

(b) Prove that if I and J are finitely generated ideals of R, then $I + J$ is also finitely generated.

Proof. Assume the ideal I of R is finitely generated by the set $A = \{a_1, a_2, \cdots, a_m\}$, where $a_1, \cdots, a_m \in R$,
and the ideal J of R is finitely generated by the set $B = \{b_1, b_2, \cdots, b_n\}$, where $b_1, \cdots, b_m \in R$.
Then

$$I = (a_1, \cdots, a_m)R = (A)R$$

and

$$J = (b_1, \cdots, b_n)R = (B)R.$$

By part (a), we have $I + J$ is generated by $A \cup B$.
Since $A \cup B$ is a finite set, $I + J$ is finitely generated. □

Exercise 2. Let R be a non-zero commutative ring with identity, and let $z \in R$. Assume that z is not nilpotent. Use the following steps to prove that there is a prime ideal of R that does not contain z.

(a) Set $\Sigma := \{I \leq R \mid 1, z, z^2, \ldots \notin I\}$, partially ordered by inclusion. Prove that $\Sigma \neq \emptyset$ and that every chain in Σ has an upper bound in Σ. Use Zorn's Lemma to conclude that Σ has a maximal element K.

Proof. Let $I = \{0\}$, then $I \leq R$.
Since z is not nilpotent, $z^n \neq 0$, $\forall\, n \in \mathbb{Z}^{\geq 0}$.
So $z^n \notin I, \forall\, n \in \mathbb{Z}^{\geq 0}$.
Thus, $I \in \Sigma$ and then $\Sigma \neq \emptyset$.

Next we show every chain in Σ has an upper bound in Σ.
Let $\mathcal{C}$ be a chain in Σ.
Set

$$I = \bigcup_{J \in \mathcal{C}} J.$$

Since $(\Sigma, \subseteq)$ is a poset,

$$I \leq R.$$

Suppose there exists at least one $z^n \in I$ for some $n \in \mathbb{Z}^{\geq 0}$.
Then $z^n \in J$ for some $J \in \mathcal{C} \subseteq \Sigma$.
Since $J \in \Sigma$, $z^n \notin J, \forall\, n \in \mathbb{Z}^{\geq 0}$.
So there is a contradiction.
Then

$$z^n \notin I, \forall\, n \in \mathbb{Z}^{\geq 0}.$$

So

$$I \in \Sigma.$$

Also

$$\forall\, J \in \mathcal{C}, J \subseteq I.$$

Thus, I is an upper bound for $\mathcal{C}$ in Σ.
By Zorn's lemma, Σ has a maximal element K. □

(b) Prove that K is prime as follows.

(1) Suppose that $r, s \in R - K$ are such that $rs \in K$. Show that $K \subsetneq K + rR \leq R$ and $K \subsetneq K + sR \leq R$.

Proof. Since $0_R \in R$,

$$K = K + r0_R \subseteq K + rR.$$

Assume $K = K + rR$.
Since $1_R \in R$,

$$K + r = K + r1_R \subseteq K + rR = K.$$

By part (a), we already have $K \leq R$, so $r \in K$.
As a result, there is a contradiction since $r \in R - K$ by assumption.
Therefore,

$$K \subsetneq K + rR. \tag{3}$$

Since R is CRW1, $rR = (r)R \leq R$.
Also, $K \leq R$.
So

$$K + rR \leq R. \tag{4}$$

By (3) and (4),

$$K \subsetneq K + rR \leq R.$$

Similarly,

$$K \subsetneq K + sR \leq R.$$

$\square$

(2) Conclude that there are $m, n \in \mathbb{Z}^{\geq 0}$ such that $z^m \in K + rR$ and $z^n \in K + sR$.

Proof. Assume $z^m \notin K + rR, \forall\ m \in \mathbb{Z}^{\geq 0}$.
Since $K + rR \leq R$, we have

$$K + rR \in \Sigma.$$

Since K is the maximal element of Σ, $K + rR \subseteq K$.
So there is a contradiction since $K \subsetneq K + rR$.
Thus, $\exists\ m \in \mathbb{Z}^{\geq 0}$ such that $z^m \in K + rR$.
Similarly, $\exists\ n \in \mathbb{Z}^{\geq 0}$ such that $z^n \in K + sR$.

$\square$

(3) Deduce that $z^{m+n} \in K$, derive a contradiction, and conclude that K is prime.

Proof. Since $z^m \in K + rR$ and $z^n \in K + sR$, there exists $k_1, k_2 \in K$ and $p_1, p_2 \in R$ such that $z^m = k_1 + rp_1$ and $z^n = k_2 + sp_2$.
Since R is CRW1,

$$\begin{aligned} z^{m+n} &= (z^m)(z^n) \\ &= (k_1 + rp_1)(k_2 + sp_2) \\ &= k_1k_2 + k_1(sp_2) + k_2(rp_1) + rs(p_1p_2) \end{aligned}$$

Since $r, s, p_1, p_2 \in R$, we have

$$sp_2, rp_1, p_1p_2 \in R.$$

Since $K \leq R$ and $k_1, k_2, rs \in K$, we have

$$k_1k_2, k_1(sp_2), k_2(rp_1), rs(p_1p_2) \in K.$$

Then

$$k_1k_2 + k_1(sp_2) + k_2(rp_1) + rs(p_1p_2) \in K.$$

So for $m, n \in \mathbb{Z}^{\geq 0}$, we have

$$z^{m+n} \in K.$$

Since $K \in \Sigma$, we have $z^n \notin K, \forall\ n \in \mathbb{Z}^{\geq 0}$, which is contradicted by $z^{m+n} \in K$.
So our assumption does not holds.
Thus, $\forall\ r, s \in R - K$, $rs \notin K$.
Henceforth, K is prime.
As a result, there is a prime ideal K of R that does not contain z. $\square$

Exercises 13-2

Exercise 3. Let $i = \sqrt{-1} \in \mathbb{C}$, and consider the following subrings of $\mathbb{C}$.

$$\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\}$$
$$\mathbb{Q}[i] := \{a + bi \mid a, b \in \mathbb{Q}\}$$

Prove that $\mathbb{Q}[i]$ is isomorphic to the field of fractions of $\mathbb{Z}[i]$.

Proof. Let $R = \mathbb{Z}[i]$ and $S = \mathbb{Q}[i]$.
By the Theorem 7.5.9, there exists well-defined ring monomorphsim

$$\begin{aligned} \rho : R &\to D^{-1}R \\ r &\mapsto \frac{rd}{d},\ d \in D \end{aligned}$$

We know S is a field in Chapter 1, so S is an integral domain.
By the subring test, we have R is a subring of S.
Also $1_S = 1_{\mathbb{R}} \in R$, we have R is an integral domain.
Let $D = R \setminus 0$, then $D^{-1}S$ is the field of fractions of R.
Define

$$\begin{aligned} \phi : R &\to S \\ r &\mapsto r \end{aligned}$$

Since ϕ is an identity map from integral domain R to integral domain S and $R \subseteq S$, ϕ is well-defined.
$\forall\ r, s \in R$,

$$\begin{aligned} \phi(r + s) &= r + s = \phi(r) + \phi(s) \\ \phi(rs) &= rs = \phi(r)\phi(s), \end{aligned}$$

it is a ring homomorphism.
Also S is CRW1 since it is an integral domain.
Since S is a field, it is a division ring and then $S^\times = S \setminus 0$.
Since $R \subseteq S$,

$$\phi(D) = D = R \setminus 0 \subseteq S \setminus 0 = S^\times.$$

By the Universal Mapping Proerty, there exists a unque well-defined ring homomorphism

$$\begin{aligned} \Phi : D^{-1}R &\to S \\ \frac{r}{d} &\mapsto \frac{\phi(r)}{\phi(d)} = \frac{r}{d},\ d \in D, r \in R. \end{aligned}$$

such that $\Phi \circ \rho = \phi$.
Let $\frac{r}{d} \in D^{-1}R$, where $r \in R$ and $d \in D$.

$$\frac{r}{d} \in \operatorname{Ker}(\Phi) \Longleftrightarrow \frac{r}{d} = 0.$$

So Φ is 1-1.
Let $a + bi \in S$, where $a, b \in \mathbb{Q}$.
Then $\exists\ s, t, p, q \in \mathbb{Z}$ and $t, q \neq 0$ such that $\frac{s}{t} = a$ and $\frac{p}{q} = b$.
Since $sq, pt \in \mathbb{Z}$,

$$sq + pti \in R$$

Since $tq \in \mathbb{Z}$ and $tq \neq 0$, we have $tq \in \mathbb{Z} \setminus 0 = D$.
So

$$\frac{sq + pti}{tq} \in D^{-1}R$$

Since

$$\phi\left(\frac{sq + pti}{tq}\right) = \frac{sq + pti}{tq} = \frac{s}{t} + \frac{p}{q}i = a + bi,$$

ϕ is onto.
Thus, ϕ is an isomomorphism.
Therefore,

$$\mathbb{Q}[i] = S \cong D^{-1}R.$$

Since $R = \mathbb{Z}[i]$, we have
$\mathbb{Q}[i]$ is isomorphic to the field of fractions of $\mathbb{Z}[i]$. $\square$

Exercise 4. Let R be an integral domain and consider the ring homomorphism $\psi\colon \mathbb{Z} \to R$ given by $\psi(n) = n \cdot 1_R$. (You do not need to show that this is a well-defined ring homomorphism.)

(a) Prove that $\operatorname{Ker}(\psi) = 0$ or $\operatorname{Ker}(\psi) = p\mathbb{Z}$ for some prime number $p \in \mathbb{Z}$.

Proof. Let $n \in \operatorname{Ker}(\psi)$.

$$n \in \operatorname{Ker}(\psi) \Longleftrightarrow n \cdot 1_R = 0_R.$$

(1) Let $|R| = \infty$.
Since R is an integral domain,

$$n \cdot 1_R = 0_R \Longleftrightarrow n = 0.$$

(2) Let $1 < |R| < \infty$ and the group $(R, +)$ not be cyclic.
Since R is an integral domain,

$$n \cdot 1_R = 0_R \Longleftrightarrow n = 0.$$

(3) Let $1 < |R| < \infty$ and the group $(R, +)$ be cyclic.
Since $\mathrm{Ker}(\psi) \subseteq \mathbb{Z}$ is a subring and the subrings of $\mathbb{Z}$ are $m\mathbb{Z}$ for all $m \in \mathbb{Z}^{\geq 0}$,

$$n \cdot 1_R = 0_R \iff n \in p\mathbb{Z} \text{ for some } p \in \mathbb{N} \text{ or } n = 0$$

Assume $\exists\, p \in 2\mathbb{Z}^{>0}$ such that $n \in p\mathbb{Z}$,

$\square$

(b) Prove that if p is a prime number such that $\mathrm{Ker}(\psi) = p\mathbb{Z}$, then R contains a finite field as a subring.

(c) Prove that if R is a field and $\mathrm{Ker}(\psi) = 0$, then R has a subring $Q \cong \mathbb{Q}$.

Proof. $\square$