Course 8

2.2 Subrings and subfields

As we have defined subgroups for groups, the most important algebraic structure with one operation, we may define analogue notion for rings or fields, algebraic structures with two operations. The principle is just the same.

Definition 2.2.1 Let $(R,+,\cdot)$ be a ring (field) and let $A \subseteq R$. Then A is called a *subring (subfield) of* R if:
(1) A is a stable subset of $(R,+,\cdot)$, that is, $\forall x,y \in A$, $x+y\,, x\cdot y \in A\,$;
(2) $(A,+,\cdot)$ is a ring (field).

We denote by $A \leq R$ and $A \leq K$ the fact that A is a subring of a ring $(R,+,\cdot)$ and a subfield of a field $(K,+,\cdot)$ respectively.

As we did for subgroups, we are looking for some characterization theorems for subrings and subfields.

Theorem 2.2.2 *Let $(R,+,\cdot)$ be a ring and $A \subseteq R$. Then $A \leq R$ if and only if*
(i) $A \neq \emptyset$ ($0 \in A$);
(ii) $x,y \in A \Longrightarrow x-y \in A$;
(iii) $x,y \in A \Longrightarrow x\cdot y \in A$.

Proof. $\Longrightarrow$. Assume that $A \leq R$. Clearly, $A \neq \emptyset$ and $x,y \in A \Longrightarrow x\cdot y \in A$. But A is stable in $(R,+)$ and $(A,+)$ is group, hence A is a subgroup of $(R,+)$. Then by the characterization theorem of subgroups we have $x,y \in A \Longrightarrow x-y \in A$.

$\Longleftarrow$. Assume that conditions (i), (ii), (iii) hold. Conditions (i) and (ii) tell us that $(A,+)$ is a subgroup of $(R,+)$ and consequently a stable subset of $(R,+)$, whereas condition (iii) assures us that A is a stable subset of $(R,\cdot)$. Now all needed properties for A to be a subring follow easily. □

Theorem 2.2.3 *Let $(K,+,\cdot)$ be a field and $A \subseteq K$. Then $A \leq K$ if and only if*
(i) $|A| \geq 2$ ($0,1 \in A$);
(ii) $x,y \in A \Longrightarrow x-y \in A$;
(iii) $x,y \in A\,, y \neq 0 \Longrightarrow x\cdot y^{-1} \in A$.

Proof. $\Longrightarrow$. Assume that A is a subfield of K. Then A is a subring of K. By Theorem 2.2.2, we have $|A| \geq 1$ and the condition (ii) holds. Since $(A,+,\cdot)$ is a field, $(A^*,\cdot)$ is a group, so that $|A^*| \geq 1$ and the condition (iii) holds.

$\Longleftarrow$. Assume that conditions (i), (ii), (iii) hold. Clearly, A is a subgroup of $(K,+)$, hence $(A,+)$ is an abelian group, and $A^* \neq \emptyset$. Moreover, since the inverse of a non-zero element is non-zero and fields do not have zero divisors, it follows that $\forall x,y \in A^*$, we have $x\cdot y^{-1} \in A^*$. Hence A^* is a subgroup of $(K^*,\cdot)$, and so $(A^*,\cdot)$ is a group. Finally, the distributive law transfers to the stable subset A of $(K,+,\cdot)$. Therefore, $A \leq K$. □

Remark 2.2.4 If A is a subring of a ring (or a subfield of a field) $(R,+,\cdot)$, then A is a subgroup of the additive group $(R,+)$ (see the conditions (i) and (ii) in Theorem 2.2.2).

We denote by $S(R,+,\cdot)$ the set of all subrings of a ring $(R,+,\cdot)$.

Example 2.2.5 (a) Every non-trivial ring $(R,+,\cdot)$ has two subrings, namely $\{0\}$ and R, called the *trivial subrings*.

(b) $\mathbb{Z}$ is a subring of $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ and $(\mathbb{C},+,\cdot)$, $\mathbb{Q}$ is a subfield of $(\mathbb{R},+,\cdot)$ and $(\mathbb{C},+,\cdot)$, $\mathbb{R}$ is a subfield of $(\mathbb{C},+,\cdot)$.

(c) The set of subrings of $(\mathbb{Z},+,\cdot)$ is $S(\mathbb{Z},+,\cdot) = \{n\mathbb{Z} \mid n \in \mathbb{N}\}$. Indeed, since every subring is a subgroup of the additive group of the ring, we have $S(\mathbb{Z},+,\cdot) \subseteq S(\mathbb{Z},+) = \{n\mathbb{Z} \mid n \in \mathbb{N}\}$. On the other hand, for each n and for every $x,y \in n\mathbb{Z}$, there exist $k,l \in \mathbb{Z}$ such that $x = nk$ and $y = nl$, whence we get $x\cdot y = n(nkl) \in n\mathbb{Z}$ and consequently, each $n\mathbb{Z}$ is a subring of $\mathbb{Z}$.
For instance, $2\mathbb{Z}$ is a subring without identity of $(\mathbb{Z},+,\cdot)$. Hence $(2\mathbb{Z},+,\cdot)$ is a ring without identity.

(d) The set $\mathbb{Z}[i] = \{x+iy \mid x,y \in \mathbb{Z}\}$ of Gauss integers is a subring of $(\mathbb{C},+,\cdot)$.

As in the case of subgroups, the intersection will be compatible with subrings, while the union will be not in general.

Theorem 2.2.6 *Let $(R,+,\cdot)$ be a ring and let $(A_i)_{i\in I}$ be a family of subrings of $(R,+,\cdot)$. Then $\bigcap_{i\in I} A_i \in S(R,+,\cdot)$.*

Proof. For each $i \in I$, $A_i \in S(R,+,\cdot)$, hence $0 \in A_i$. Then $0 \in \bigcap_{i\in I} A_i \neq \emptyset$. Now let $x, y \in \bigcap_{i\in I} A_i$. Then $x, y \in A_i$, $\forall i \in I$. But $A_i \in S(R,+,\cdot)$, $\forall i \in I$. It follows that $x-y$, $x\cdot y \in A_i$, $\forall i \in I$, hence $x-y$, $x\cdot y \in \bigcap_{i\in I} A_i$. Therefore, by Theorem 2.2.2, $\bigcap_{i\in I} A_i \in S(R,+,\cdot)$. □

Example 2.2.7 In Example 2.2.5 (c), we have seen that $S(\mathbb{Z},+,\cdot) = \{n\mathbb{Z} \mid n \in \mathbb{N}\}$. Take $A = 2\mathbb{Z}$, $B = 3\mathbb{Z} \in S(\mathbb{Z},+,\cdot)$. Then $A \cap B = 2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}$ is a subring of $(\mathbb{Z},+)$. But $A \cup B = 2\mathbb{Z} \cup 3\mathbb{Z}$ is not a subring of $(\mathbb{Z},+)$, because, for instance, we have $2, 3 \in A \cup B$, but $2+3 = 5 \notin A \cup B$. Therefore, in general the union of subrings is not a subring.

This leads to the idea of subring generated by a subset of a ring.

Definition 2.2.8 Let $(R,+,\cdot)$ be a ring and let $X \subseteq R$. Then we denote

$$< X >= \bigcap \{A \leq R \mid X \subseteq A\} \in S(R,+,\cdot)$$

and we call it the *subring generated by X*.

In fact, $< X >$ is the "least" subring of R containing X.

Here X is called the *generating set* of $< X >$.

If $X = \{x\}$, then we denote $< x >=< \{x\} >$.

Remark 2.2.9 Notice that $< \emptyset >= \{0\}$ by Definition 2.2.8.

Let us now determine how the elements of a generated subring look like.

Theorem 2.2.10 *Let $(R,+,\cdot)$ be a ring and let $\emptyset \neq X \subseteq R$. Then*

$$< X >= \left\{ \sum_{\text{finite}} \varepsilon \cdot x_1 \cdot x_2 \cdots x_n \middle| \varepsilon \in \{\pm 1\}, x_i \in X, i = 1, \ldots, n, n \in \mathbb{N}^* \right\},$$

that is, the set of all finite sums of finite products of elements in X, possibly with changed sign.

Proof. Denote by A the right hand side, that is,

$$A = \left\{ \sum_{\text{finite}} \varepsilon \cdot x_1 \cdot x_2 \cdots x_n \middle| \varepsilon \in \{\pm 1\}, x_i \in X, i = 1, \ldots, n, n \in \mathbb{N}^* \right\}.$$

We are going to prove that A is the least subring of R containing X, that is, to show the following 3 properties:

(i) $A \leq R$;

(ii) $X \subseteq A$;

(iii) If $B \leq R$ and $X \subseteq B$, then $A \subseteq B$.

Let us discuss them one by one.

(i) Clearly, we have $A \neq \emptyset$, because $X \neq \emptyset$. Let $a_1 = \sum_{\text{finite}} \varepsilon_1 \cdot x_1 \cdot x_2 \cdots x_m$ and $a_2 = \sum_{\text{finite}} \varepsilon_2 \cdot y_1 \cdot y_2 \cdots y_n \in A$. Clearly, we have $a_1 - a_2 \in A$ and $a_1 \cdot a_2 \in A$, so that $A \leq R$ by Theorem 2.2.2.

(ii) Clear.

(iii) If $B \leq R$ and $X \subseteq B$, then $\sum_{\text{finite}} \varepsilon \cdot x_1 \cdot x_2 \cdots x_n \in B$ for every $\varepsilon \in \{\pm 1\}$ and $x_1, \ldots, x_n \in X \subseteq B$ by Theorem 2.2.2. It follows that $A \subseteq B$.

Hence A is the least subring of R containing X, which shows the conclusion of the theorem. □

Theorem 2.2.11 *Let $(R,+,\cdot)$ be a ring. Then $(S(R,+,\cdot),\subseteq)$ is a complete lattice, where $\inf(A_i)_{i\in I} = \bigcap_{i\in I} A_i$ and $\sup(A_i)_{i\in I} =< \bigcup_{i\in I} A_i >$ for every family $(A_i)_{i\in I}$ of subrings of R.*

Remark 2.2.12 One may establish corresponding results on the subfield generated by a subset of a field, and on the subfield lattice of a field.

2.3 Ring homomorphisms

Let us now define some special maps between rings. Recall that we denote by the same symbol operations in different arbitrary structures.

Definition 2.3.1 Let $(R,+,\cdot)$ and $(R',+,\cdot)$ be rings and $f : R \to R'$. Then f is called a *(ring) homomorphism* if $\forall x, y \in R$ we have

$$f(x+y) = f(x) + f(y)\,,$$

$$f(x \cdot y) = f(x) \cdot f(y)\,.$$

The notions of *(ring) isomorphism*, *endomorphism* and *automorphism* are defined as usual.

Remark 2.3.2 If $f : R \to R'$ is a ring homomorphism, then the first condition from its definition tells us that f is a group homomorphism between $(R,+)$ and $(R',+)$. Then f takes the identity element of $(R,+)$ to the identity element of $(R',+)$, that is, $f(0) = 0'$ and we also have $f(-x) = -f(x)$, $\forall x \in R$. But in general, even if R and R' have identities, denoted by 1 and $1'$ respectively, in general it does not follow that a ring homomorphism $f : R \to R'$ has the property that $f(1) = 1'$.

We denote by $R \simeq R'$ or $R \cong R'$ the fact that two rings R and R' are isomorphic.

Example 2.3.3 (a) Let $(R,+,\cdot)$ and $(R',+,\cdot)$ be rings and let $f : R \to R'$ be defined by $f(x) = 0'$, $\forall x \in R$. Then f is a homomorphism, called the *trivial homomorphism*.

Notice that if R and $R' \neq \{0'\}$ have identities, we do not have $f(1) = 1'$.

(b) Let $(R,+,\cdot)$ be a ring. Then the identity map $1_R : R \to R$ is an automorphism of R.

(c) Let $(R,+,\cdot)$ be a ring and let $A \leq R$. Define $i : A \to R$ by $i(x) = x$, $\forall x \in A$. Then i is a homomorphism, called the *inclusion homomorphism*.

(d) The map $f : \mathbb{R} \to M_2(\mathbb{R})$ defined by $f(x) = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$, $\forall x \in \mathbb{R}$, is a ring homomorphim between the rings $(\mathbb{R},+,\cdot)$ and $(M_2(\mathbb{R}),+,\cdot)$.

Theorem 2.3.4 *(i) Let $f : R \to R'$ be a ring isomorphism. Then $f^{-1} : R' \to R$ is again a ring isomorphism.*

(ii) Let $f : R \to R'$ and $g : R' \to R''$ be ring homomorphisms. Then $g \circ f : R \to R''$ is a ring homomorphism.

Proof. Homework.

Definition 2.3.5 Let $(R,+,\cdot)$ and $(R',+,\cdot)$ be rings with identity elements 1 and $1'$ respectively and let $f : R \to R'$ be a ring homomorphism. Then f is called a *unitary homomorphism* if $f(1) = 1'$.

Theorem 2.3.6 *Let $(R,+,\cdot)$ and $(R',+,\cdot)$ be rings with identity elements 1 and $1'$ respectively and let $f : R \to R'$ be a ring homomorphism.*

(i) If f is surjective, then f is unitary.

(ii) If f is unitary and $x \in R$ has an inverse element $x^{-1} \in R$, then $f(x)$ has an inverse and

$$(f(x))^{-1} = f(x^{-1})\,.$$

Proof. (i) Let $x' \in R'$. Then $\exists x \in R$ such that $f(x) = x'$, because f is surjective. Then we have

$$x' \cdot f(1) = f(x) \cdot f(1) = f(x \cdot 1) = f(x) = x'\,,$$

$$f(1) \cdot x' = f(1) \cdot f(x) = f(1 \cdot x) = f(x) = x'\,,$$

hence $f(1) = 1'$ is the identity element of R'.

(ii) Since

$$x \cdot x^{-1} = x^{-1} \cdot x = 1 \Longrightarrow f(x \cdot x^{-1}) = f(x^{-1} \cdot x) = f(1) \Longrightarrow$$

$$\Longrightarrow f(x) \cdot f(x^{-1}) = f(x^{-1}) \cdot f(x) = 1'\,,$$

it follows that $(f(x))^{-1} = f(x^{-1})$. □

Let us now define two important sets related to a ring homomorphism, that will be even subrings.

Definition 2.3.7 Let $f : R \to R'$ be a ring homomorphism. Then the set

$$\mathrm{Ker}f = \{x \in R \mid f(x) = 0'\}$$

is called the *kernel* of the homomorphism f and the set

$$\mathrm{Im}f = \{f(x) \mid x \in R\}$$

is called the *image* of the homomorphism f.

Theorem 2.3.8 *Let $f : R \to R'$ be a ring homomorphism. Then* $\mathrm{Ker}f \leq R$ *and* $\mathrm{Im}f \leq R'$.

Proof. Since $f(0) = 0'$, we have $0 \in \mathrm{Ker}f \neq \emptyset$. Now let $x, y \in \mathrm{Ker}f$. Then $f(x) = f(y) = 0'$. It follows that

$$f(x - y) = f(x) + f(-y) = f(x) - f(y) = 0' - 0' = 0',$$
$$f(x \cdot y) = f(x) \cdot f(y) = 0' \cdot 0' = 0',$$

hence $x - y, x \cdot y \in \mathrm{Ker}f$. Therefore, $\mathrm{Ker}f \leq R$.

Since $0' = f(0)$, we have $0' \in \mathrm{Im}f \neq \emptyset$. Now let $x', y' \in \mathrm{Im}f$. Then $\exists x, y \in G$ such that $f(x) = x'$ and $f(y) = y'$. It follows that

$$x' - y' = f(x) - f(y) = f(x - y) \in \mathrm{Im}f,$$

$$x' \cdot y' = f(x) \cdot f(y) = f(x \cdot y) \in \mathrm{Im}f,$$

hence $x' - y', x' \cdot y' \in \mathrm{Im}f$. Therefore, $\mathrm{Im}f \leq R'$. □

Theorem 2.3.9 *Let $f : R \to R'$ be a ring homomorphism. Then* $\mathrm{Ker}f = \{0\} \iff f$ *is injective*.

Proof. $\Longrightarrow$. Suppose that $\mathrm{Ker}f = \{0\}$. Let $x, y \in R$ be such that $f(x) = f(y)$. Then $f(x) - f(y) = 0'$, whence it follows that $f(x - y) = 0'$, that is, $x - y \in \mathrm{Ker}f = \{0\}$. Hence $x = y$. Therefore, f is injective.

$\Longleftarrow$. Suppose that f is injective. Clearly, $\{0\} \subseteq \mathrm{Ker}f$. Now let $x \in \mathrm{Ker}f$. Then $f(x) = 0' = f(0)$, whence $x = 0$. Hence $\mathrm{Ker}f \subseteq \{0\}$, so that $\mathrm{Ker}f = \{0\}$. □