24. Rings

24.1. **Definitions and basic examples.**

Definition. A ring R is a set with two binary operations $+$ (addition) and $\cdot$ (multiplication) satisfying the following axioms:

(A0) R is closed under addition
(A1) addition is associative
(A2) there exists $0 \in R$ s.t. $a + 0 = 0 + a$ for all $a \in R$
(A3) for every $a \in R$ there exists $-a \in R$ s.t. $a + (-a) = (-a) + a = 0$
(A4) addition is commutative
(M0) R is closed under multiplication
(M1) multiplication is associative
(D1) distributivity on the left: $(a + b)c = ac + bc$ for all $a, b, c \in R$
(D2) distributivity on the right: $c(a + b) = ca + cb$ for all $a, b, c \in R$

Remark: The axioms (A0)-(A3) simply say that R is a group with respect to addition. Axiom (A4) says that the group $(R, +)$ is abelian.

Definition. A ring R is called commutative if multiplication is commutative, that is, $ab = ba$ for all $a, b \in R$.

Definition. A ring R is a called a ring with 1 (or a ring with unity) if there exists $1 \in R$ s.t. $a \cdot 1 = 1 \cdot a = a$ for all $a \in R$.

Definition. A ring R is called a field if

(i) R is commutative,
(ii) R is a ring with 1
(iii) for every $a \in R$, with $a \neq 0$, there exists $a^{-1} \in R$ such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$
(iv) $1 \neq 0$.

Examples: 1. Fields. The examples of fields we know so far are $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ and $\mathbb{Z}_p$ where p is prime.

2. Commutative rings with 1, which are not fields. The examples we have seen so far are $\mathbb{Z}$ and $\mathbb{Z}_n$ where n is non-prime. Another important class of examples is given by polynomial rings:

Let R be a commutative ring with 1, and let $R[x]$ denote the set of all polynomials with coefficients in R. One can think of $R[x]$ as the set of formal

expressions $a_0 + a_1x + \ldots + a_nx^n$, with $a_i \in R$. Addition and multiplication on $R[x]$ are defined according to the "usual algebra rules", e.g.

$$(a_0 + a_1x) + (b_0 + b_1x + b_2x^2) = (a_0 + b_0) + (a_1 + b_1)x + b_2x^2 \text{ and}$$

$$(a_0+a_1x)\cdot(b_0+b_1x+b_2x^2) = a_0b_0+(a_0b_1+a_1b_0)x+(a_0b_2+a_1b_1)x^2+a_1b_2x^3.$$

It is a rather long but straightforward calculation to check that $R[x]$ with these operations becomes a ring with 1. The unity element of $R[x]$ is the constant polynomial 1 (where 1 is the unity element of R).

3. Commutative rings without 1. The basic examples are the rings $n\mathbb{Z}$ where $n \geq 2$ is a fixed integer.

4. Noncommutative rings. The basic examples are the matrix rings $Mat_n(F)$ where F is some field and $n \geq 2$.

In this course we will be mostly interested in the structure of commutative rings with 1.

24.2. **Subrings.** A common way to construct more rings is to take subrings of rings we already know. As in the case of subgroups, we have two definitions of a subring – the first one is conceptually natural while the second one which is easy to understand and apply.

Definition 1. Let R be a ring. A subset S is called a subring of R if S is a ring with respect to addition and multiplication defined on R.

Definition 2. Let R be a ring. A subset S is called a subring of R if

(i) S contains 0
(ii) S is closed under addition
(iii) S is closed under additive inversion, that is, if $x \in S$, then $-x \in S$
(iv) S is closed under multiplication

Note that conditions (i)-(iii) simply say that S is a subgroup of $(R, +)$, that is, a subgroup of R with respect to addition.

The equivalence of Definitions 1 and 2 is proved similarly to the case of subgroups. Here we just mention that condition (i) comes from axiom (A2), (ii) comes from axiom (A0), (iii) comes from (A3) and (iv) comes from (M0). The remaining axioms (A1), (M1), (D1) and (D2) do not yield any extra conditions since if they hold for R, they automatically hold for any subset of R.

Example 1: Let $R = \mathbb{R}$ (reals) and $S = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$.

(a) Prove that S is a subring of R

(b) Prove that S is the minimal subring of R containing 1 and $\sqrt{2}$. In other words, prove that if T is any subring of R containing 1 and $\sqrt{2}$, then $S \subseteq T$.

Proof of (a). Let us check conditions (i)-(iv):

(i) Since $0 = 0 + 0 \cdot \sqrt{2}$ and $0 \in \mathbb{Z}$, we have $0 \in S$.

(ii) Let $x, y \in S$. Then $x = a + b\sqrt{2}$ and $y = c + d\sqrt{2}$ for some $a, b, c, d \in \mathbb{Z}$. Then $x + y = (a + c) + (b + d)\sqrt{2}$. Since $a, b, c, d \in \mathbb{Z}$, we have $a + c, b + d \in \mathbb{Z}$ as well, so $x + y \in S$, as desired.

(iii) Let $x \in S$, so that $x = a + b\sqrt{2}$ for some $a, b \in \mathbb{Z}$. Then $-x = -a + (-b)\sqrt{2}$. Since $-a, -b \in \mathbb{Z}$, we conclude that $-x \in S$.

(iv) Let $x, y \in S$, so that $x = a + b\sqrt{2}$ and $y = c + d\sqrt{2}$ for some $a, b, c, d \in \mathbb{Z}$. Then $xy = ac + ad\sqrt{2} + bc\sqrt{2} + 2bd = (ac + 2bd) + (ad + bc)\sqrt{2} = e + f\sqrt{2}$ where $e = ac + 2bd$ and $f = ad + bc$. Since $e, f \in \mathbb{Z}$, we conclude that $xy \in S$.

Thus, we proved that S is a subring of R. □

Proof of (b). Let T be any subring of R containing 1 and $\sqrt{2}$.

(α) Since T is closed under addition, T must contain $1+1, 1+1+1, \ldots$, so T contains all positive integers

(β) Since T is closed under additive inversion, by (α), T contains all negative integers.

(γ) We also know that $0 \in T$, so from (α) and (β) we obtain that T contains $\mathbb{Z}$.

(δ) Since T contains $\mathbb{Z}$ and $\sqrt{2}$ and T is closed under multiplication, we conclude that T contains $b\sqrt{2}$ for all $b \in \mathbb{Z}$.

(ε) Since T is closed under addition, from (γ) and (δ) we get that T contains $a + b\sqrt{2}$ for all $a, b \in \mathbb{Z}$, so T contains S.

□

Let us now consider a general problem.

Problem 24.1. *Let R be a commutative ring and Y a subset of R. Find the minimal subring of R containing Y.*

In Example 1 we solved this problem with $R = \mathbb{R}$ and $Y = \{1, \sqrt{2}\}$. However, we had an advantage of knowing the answer right away, and we only had to prove that the given answer was correct. Here is a very general three-step algorithm which can be used to solve Problem 24.1 when the answer is not known.

Algorithm for solving Problem 24.1.

Step 1. Make a guess. Your guess should be the set of all elements of R which can be obtained from Y using addition, additive inversion and multiplication.

Step 2. Let S be your guess from Step 1. Prove that S is a subring.

Step 3. Prove that if T is any subring of R containing Y, then $S \subset T$.

Steps 2 and 3 imply that S is the minimal subring of R containing Y.

Example 2: Let $R = \mathbb{R}[x]$, the polynomials with real coefficients. Find the minimal subring of R which contains x^2.

Solution: We implement the above algorithm. In this example $Y = \{x^2\}$.

Step 1: What can we get starting from x^2 if we are only using addition, additive inversion and multiplication? Using multiplication, we get $x^2 \cdot x^2 = x^4$, $x^4 \cdot x^2 = x^6, \ldots$. So, we get x^{2k} for every $k \in \mathbb{Z}_{>0}$.
Next, for a fixed k, using addition and additive inversion from x^{2k} we get $0, \pm x^{2k}, \pm 2x^{2k}, \ldots$, so we can get $a_{2k}x^{2k}$ for any $a_{2k} \in \mathbb{Z}$ (note that 0 can be obtained, for instance, as $x^{2k} + (-x^{2k})$).
Finally, adding such elements for different $k's$ we get any polynomial of the form

$$a_2x^2 + a_4x^4 + \ldots + a_{2n}x^{2n} \text{ where each } a_{2i} \in \mathbb{Z} \text{ and } n \in \mathbb{Z}_{>0}. \qquad (***)$$

It seems that no other elements can be created using addition, additive inversion and multiplication. Thus we take the set of all polynomials given by (***) as our guess.

Step 2: Let

$$S = \{a_2x^2 + a_4x^4 + \ldots + a_{2n}x^{2n} \text{ where each } a_{2i} \in \mathbb{Z} \text{ and } n \in \mathbb{Z}_{>0}\}.$$

We need to prove that S is a subring. This is done by direct verification of conditions (i)-(iv), similarly to what we did in Example 1.

Exercise: Do this verification. It is routine, but without it you would not know if you are getting correct answer or not!!!

Step 3: Prove that if T is any subring containing x^2, then T contains S. To prove this we essentially repeat our argument from Step 1.

So, here is our final answer. The minimal subring of $\mathbb{R}[x]$ containing x^2 is

$$\{a_2x^2 + a_4x^4 + \ldots + a_{2n}x^{2n} \text{ where each } a_{2i} \in \mathbb{Z} \text{ and } n \in \mathbb{Z}_{>0}\}.$$

What if the guess is wrong. Note that the argument in Step 1 does not have to be formal. Step 1 is just used to make a guess, and all justification is done in Steps 2 and 3. So, what happens if our guess S from Step 1 was wrong? In other words, let S_{min} be the correct answer to the problem, that

is, let S_{min} be the minimal subring of R containing Y, and suppose that our guess S is not equal to S_{min}. Then one of the following must happen:

(i) S contains some redundant element, that is, there exists some $f \in S$ s.t. $f \notin S_{min}$.

(ii) S does not have any redundant elements, but some elements are missing from S. In other words, S is contained in S_{min}, but $S \neq S_{min}$.

In both cases we will be able to detect the mistake in Step 2 or 3. If problem (i) occurred, then we will not be able to complete Step 3, that is, we will not be able to prove that if T is any subring of R containing Y, then T contains S. If problem (ii) occurred, then we will not be able to complete Step 2, that is, we will not be able to prove that S is a subring.

Here is an illustration of two typical wrong guesses in Example 2.

Wrong guess 1. $S = \{ax^2 : a \in \mathbb{Z}\}$ (recall that this was our initial guess in class). Here problem (ii) occurs. We detect this problem in Step 2 as S is clearly not a subring: $x^2 \in S$, but $x^4 = x^2 \cdot x^2 \notin S$.

Wrong guess 2.

$$S = \{a_2x^2 + a_4x^4 + \ldots + a_{2n}x^{2n} \text{ where each } a_{2i} \in \mathbb{R} \text{ and } n \in \mathbb{Z}_{>0}\}$$

(the difference with the correct answer is that here coefficients are allowed to be real numbers, not necessarily integers). Here problem (i) occurs. We detect this problem in Step 3. For instance, starting from the assumption that T is a subring and $x^2 \in T$, we will never be able to prove that $\frac{1}{2}x^2 \in T$, so we cannot deduce that T contains S.

Let us now go back to our solution in Example 2. Note that when we made our guess S in Step 1, we made sure that problem (i) did not occur, that is, for every element f that we included in S, we showed explicitly how to obtain that element starting from x^2 using addition, additive inversion and multiplication. This is why in Step 3 we did not have to do any new computations and simply referred to work already done in Step 1. This is how things would usually work out. However, in some examples it may be convenient to make a "more risky" guess. In such cases we will need to do Step 3 carefully, as we did in Example 1.