

Chapter 11: Rings

11.1: Definition of a Ring

- **Ring:** A *ring* R is a set with two laws of composition $+$ and \times , called addition and multiplication, that satisfy these axioms:
 - (a) With the law of composition $+$, R is an abelian group that we denote by R^+ ; its identity is denoted by 0 .
 - (b) Multiplication is commutative and associative, and has an identity denoted by 1 .
 - (c) *Distributive law:* For all a, b and c in R , $(a + b)c = ac + bc$.
- **Subring:** Subset which is closed under addition, subtraction, multiplication and which contains 1 .
- **Non-commutative Ring:** Satisfies all of the above axioms, except for the commutative law for multiplication.
- **Gauss integers:** The complex numbers of the form $a + bi$ where a and b are integers form a subring of \mathbb{C} that we denote by $\mathbb{Z}[i] = \{a + bi \mid b, b \in \mathbb{Z}\}$. Its elements are points of a square lattice in the complex plane.
 - $\mathbb{Z}[\alpha]$ **subring:** Contains every complex number $\beta = a_n\alpha^n + \cdots + a_1\alpha + a_0$ where a_i are in \mathbb{Z} and α is a complex number.
 - * Analogous to the ring of Gauss integers.
 - * Subring generated by α
 - * Usually not represented as a lattice in the complex plane
- A complex number α is **algebraic** if it is a root of a (nonzero) polynomial with integer coefficients (i.e. if some expression of the form $a_n\alpha^n + \cdots + a_1\alpha + a_0$ evaluates to 0)
 - When α is algebraic there will be many polynomial expressions that represent the same complex number.
- If there is no polynomial with integer coefficients having α as a root, α is **transcendental**
 - When α is transcendental, two distinct polynomial expressions represent distinct complex numbers, and the elements of the ring $\mathbb{Z}[\alpha]$ correspond bijectively to polynomials $p(x)$ with integer coefficients.
- A polynomial in x with coefficients in a ring R is an expression of the form

$$a_n x^n + \cdots + a_1 x + a_0$$

with a_i in R .

- **Zero Ring:** A ring containing only the element 0.
 - A ring R in which the elements 1 and 0 are equal is the zero ring.
- **Unit:** A *unit* of a ring is an element that has a multiplicative inverse (if it exists, it is unique)
 - Units in the ring of integers are 1 and -1
 - Units in the ring of Gauss integers are ± 1 and $\pm i$
 - Units in the ring $\mathbb{R}[x]$ of real polynomials are the nonzero constant polynomials
 - The identity element 1 of a ring is always a unit

11.2: Polynomial Rings

- **Formal Polynomial:** A polynomial with coefficients in a ring R is a (finite) linear combination of powers of the variable: $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ where the coefficients a_i are elements of R .
 - The set of polynomials with coefficients in a ring R will be denoted $R[x]$
 - Thus $\mathbb{Z}[x]$ is the set of *integer polynomials*
- The *monomials* x^i are considered independent, so if \exists another polynomial with coefficients in R , then $f(x) = g(x)$ only if $a_i = b_i$ for all $i = 0, 1, 2, \dots$
- **Degree:** The *degree* of a nonzero polynomial (denoted $\deg f$) is the largest integer n such that the coefficient a_n of x_n is not zero
 - A polynomial of degree zero is called a *constant* polynomial
 - The zero polynomial is also a constant polynomial, but its degree will not be defined
- **Leading Coefficient:** The nonzero coefficient of highest degree of a polynomial
 - **Monic Polynomial:** Polynomial with a leading coefficient of 1
- A polynomial is determined by its vector of coefficients a_i : $a = (a_0, a_1, \dots)$ where a_i are elements of R , all but a finite number zero.
- When R is a field, these infinite vectors form the vector space Z with the infinite basis e_i . The vector e_i corresponds to the monomial x_i , and the monomials form a basis of the space of all polynomials.

- **Addition of polynomials:** $f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \dots$ where $(a_i + b_i)$ is addition in R
- **Multiplication of polynomials:** $f(x)g(x) = (a_0 + a_1x + \dots)(b_0 + b_1x + \dots)$ where $a_i b_j$ are to be evaluated in the ring R .
- There is a unique commutative ring structure on the set of polynomials $R[x]$ having these properties:
 - Additions of polynomials as defined above
 - Multiplication of polynomials as defined above
 - The ring R becomes a subring of $R[x]$ when the elements of R are identified with the constant polynomials
- **Division with Remainder:** Let R be a ring, f is a monic polynomial, and g is any polynomial, both with coefficients in R . There are uniquely determined polynomials q and r in $R[x]$ s.t. $g(x) = f(x)q(x) + r(x)$ where r has degree ≥ 0 and $\leq \deg f$
 - Division with remainder can be done whenever the leading coefficient of f is a unit
 - If $g(x)$ is a polynomial in $R[x]$ and α is an element of R , the remainder of division of $g(x)$ by $x - \alpha$ is $g(\alpha)$. Thus $x - \alpha$ divides g in $R[x]$ iff $g(\alpha) = 0$
- **Monomial:** a formal product of some variables x_1, \dots, x_n of the form

$$x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$$

where i_v are non-negative integers.

- **Degree:** the sum $i_1 + \dots + i_n$, sometimes called *total degree*
- **Multi-index:** an n -tuple that can be represented with vector notation e.g. $i = (i_1, \dots, i_n)$.
- A monomial can be written as $x^i = x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$ using multi-index form
- The monomial x^0 is denoted by 1
- With multi-index notation, a polynomial $f(x) = f(x_1, \dots, x_n)$ can be written in exactly one way in the form

$$f(x) = \sum_i a_i x^i$$

where i runs through all multi-indices (i_1, \dots, i_n) , the coefficients a_i are in R and only finitely many of these coefficients are not 0.

- **Homogeneous Polynomial:** A polynomial in which all monomials with nonzero coefficients have degree d

11.3: Homomorphisms and Ideals

- **Ring Homomorphism:** A *ring homomorphism* $\phi : R \rightarrow R'$ is a map from one ring to another which is compatible with the laws of composition and which carries the unit element 1 of R to the unit element 1 of R' - a map such that for all a and b in R ,

$$\phi(a + b) = \phi(a) + \phi(b), \quad \phi(ab) = \phi(a)\phi(b), \quad \text{and} \quad \phi(1) = 1$$

- The map $\phi : \mathbb{Z} \rightarrow \mathbb{F}_p$ that send an integer to its congruence class modulo p is a ring homomorphism.

- **Isomorphism:** An *isomorphism* of rings is a bijective homomorphism, denoted $R \approx R'$
- Evaluation of real polynomials at a real number a defines a homomorphism

$$\mathbb{R}[x] \rightarrow \mathbb{R}, \quad \text{that sends} \quad p(x) \rightsquigarrow p(a)$$

- **Substitution Principle:** Let $\phi : R \rightarrow R'$ be a ring homomorphism, and let $R[x]$ be the ring of polynomials with coefficients in R .
 - (a) Let α be an element of R' . There is a unique homomorphism $\Phi : R[x] \rightarrow R'$ that agrees with the map ϕ on constant polynomials, and that send $x \rightsquigarrow \alpha$
 - (b) Given elements $\alpha_1, \dots, \alpha_n$ of R' , there is a unique homomorphism $\Phi : R[x_1, \dots, x_n] \rightarrow R'$, from the polynomial ring in n variables to R' , that agrees with ϕ on constant polynomials and that send $x_v \rightsquigarrow \alpha_v$, for $v = 1, \dots, n$.
- Let R be any ring, and let P be the polynomial ring $R[x]$. One can use the substitution principle to construct an isomorphism

$$R[x, y] \rightarrow P[y] = (R[x])[y]$$

This statement is a formalization of the procedure of collecting terms of like degree in y in a polynomial $f(x, y)$. For example:

$$x^4y + x^3 - 3x^2y + y^2 + 2 = y^2 + (x^4 - 3x^2)y + (x^3 + 2)$$

- Let $x = (x_1, \dots, x_m)$ and $y = (y_1, \dots, y_n)$ denote sets of variables. There is a unique isomorphism $R[x, y] \rightarrow R[x][y]$, which is the identity on R and sends the variables to themselves.
- Let $f(x, y)$ and $g(x, y)$ be polynomials in two variables, elements of $R[x, y]$. Suppose that f is a monic polynomial of degree m (grouped by y). There are uniquely determined polynomials $q(x, y)$ and $r(x, y)$ such that $g = fq + r$ and $0 \leq r(x, y) < m$

- There is exactly one homomorphism $\phi : \mathbb{Z} \rightarrow R$, defined for $n \geq 0$ where $\phi(n) = 1 + \cdots + 1$ (for n terms) and $\phi(-n) = -\phi(n)$

- **Kernel:** The *kernel* of ϕ is the set of elements R that map to zero:

$$\ker\phi = \{s \in R \mid \phi(s) = 0\}$$

- If s is in $\ker\phi$, then for every element r of R , rs is in $\ker\phi$

- **Ideal:** An *ideal* I of a ring R is a nonempty subset of R with these properties:

- (a) I is closed under addition, and
- (b) If s is in I and r is in R , then rs is in I

- **Principal Ideal:** The ideal formed by multiples of a particular element a , also defined as:

$$(a) = aR = Ra = \{ra \mid r \in R\}$$

- **Unit Ideal:** The ring R is the principal ideal (1) , and is called the *unit ideal*
- **Zero Ideal:** The principal ideal (0)
- **Proper Ideal:** An ideal that is neither the unit or zero ideal

- The kernel of a ring homomorphism is an ideal
- An ideal is not a subring unless the ideal I is equal to the whole ring R
- The ideal *generated by a set of elements* $\{a_1, \dots, a_n\}$ of a ring R is the smallest ideal that contains those elements. This ideal is often denoted as (a_1, \dots, a_n) :

$$(a_1, \dots, a_n) = \{r_1a_1 + \cdots + r_na_n \mid r_i \in R\}$$

- The only ideals of a field are the zero ideal and the unit ideal
- A ring that has exactly two ideals is a field
- Every homomorphism $\phi : F \rightarrow R$ from a field F to a nonzero ring R is injective
- The ideals in the ring of integers are the subgroups of \mathbb{Z}^+ , and they are principal ideals
- Every ideal in the ring $F[x]$ of polynomials in one variable x over a field F is a principal ideal. A nonzero ideal I in $F[x]$ is generated by the unique monic polynomial of lower degree that it contains.
- Let f be a monic integer polynomial, and let g be another integer polynomial. If $f \mid g$ in $\mathbb{Q}[x]$, $f \mid g$ in $\mathbb{Z}[x]$

- **Greatest Common Divisor:** Let R denote the polynomial ring $F[x]$ in one variable over a field F , and let f and g be elements of R , not both zero. Their *greatest common divisor* $d(x)$ is the unique monic polynomial that generates the ideal (f, g) . It has these properties:
 - (a) $Rd = Rf + Rg$
 - (b) d divides f and g
 - (c) If a polynomial $e = e(x)$ divides both f and g , it also divides d
 - (d) There are polynomials p and q such that $d = pf + qg$
- **Characteristic:** The non-negative integer n that generates the kernel of the homomorphism $\phi : \mathbb{Z} \rightarrow R$
 1. If $n = 0$, this means that no positive multiple of 1 in R is equal to zero. Otherwise n is the smallest positive integer s.t. " n times 1" is zero in R

11.4: Quotient Rings

- Let I be an ideal of a ring R . There is a unique ring structure on the set \bar{R} (R/I) of additive cosets of I such that the map $\pi : R \rightarrow \bar{R}$ that send $a \rightsquigarrow \bar{a} = [a + I]$ (the coset generated with the subgroup I) is a ring homomorphism. The kernel of π is I .
 - **Canonical Map:** π
 - **Quotient Ring:** \bar{R}
 - **Residue:** The image \bar{a} of a
- **Mapping Property of Quotient Rings:** Let $f : R \rightarrow R'$ be a ring homomorphism with kernel K and let I be another ideal. Let $\pi : R \rightarrow \bar{R}$ be the canonical map from R to $\bar{R} = R/I$
 - (a) If $I \subset K$, there is a unique homomorphism $\bar{f} : \bar{R} \rightarrow R'$ such that $\bar{f}\pi = f : R \rightarrow R'$.
 - (b) **First Isomorphism Theorem:** If f is onto and $I = K$, \bar{f} is an isomorphism.
- **Correspondence Theorem:** Let $\phi : R \rightarrow \mathcal{R}$ be an onto ring homomorphism with kernel K . There is a bijective correspondence between the set of all ideals of \mathcal{R} and the set of ideals of R that contain K . It is defined as follows:
 - If I is an ideal of R and of $K \subset I$, the corresponding ideal of \mathcal{R} is $\phi(I)$
 - If \mathcal{I} is an ideal of \mathcal{R} , the corresponding ideal of R is $\phi^{-1}(\mathcal{I})$
- Of the ideal I of R corresponds to the ideal \mathcal{I} of \mathcal{R} , the quotient rings R/I and \mathcal{R}/\mathcal{I} are naturally isomorphic.

- The image of a subgroup is a subgroup
- We reinterpret the quotient ring construction when the ideal is principal ($I = (a)$). In this situation, $\bar{R} = R/I$ as the "killing" of a by imposing the relation $a = 0$ on R
 - Imposing the relation $a = 0$ on R forces us to set $b = b + ra$ for all b, r in R
 - Two elements b and b' of R have the same image in \bar{R} iff b' had the form $b + r_1a_1 + \cdots + r_na_n$ for some $r_i \in R$

11.5: Adjoining Elements

Chapter 11 Exercises

Problem 11.1.1: Prove that $7 + \sqrt[3]{2}$ and $\sqrt{3} + \sqrt{-5}$ are algebraic numbers

Proof. We need to show that they are roots of a nonzero polynomial with integer coefficients. We can show that $(7 + \sqrt[3]{2})^3 - 21(7 + \sqrt[3]{2})^2 + 147(7 + \sqrt[3]{2}) - 345 = 0$. This means it can be represented as the root of a polynomial, namely, $x^3 - 21x^2 + 147x - 345$. For $\sqrt{3} + \sqrt{-5}$, let $x = \sqrt{3} + \sqrt{-5}$.

$$\begin{aligned} x^2 &= (\sqrt{3} + \sqrt{-5})(\sqrt{3} + \sqrt{-5}) \\ x^2 &= 3 + 2\sqrt{-15} - 5 \\ x^2 &= 2\sqrt{-15} - 2 \\ x^2 + 2 &= 2\sqrt{-15} \\ (x^2 + 2)^2 &= -60 \\ (x^2 + 2)^2 + 60 &= 0 \end{aligned}$$

This means that $\sqrt{3} + \sqrt{-5}$ can be represented as the root of a polynomial. □

Problem 11.1.3: Let $\mathbb{Q}[\alpha, \beta]$ denote the smallest subring of \mathbb{C} containing the rational numbers \mathbb{Q} and the elements $\alpha = \sqrt{2}$ and $\beta = \sqrt{2}$. Let $\gamma = \alpha + \beta$. Is $\mathbb{Q}[\alpha, \beta] = \mathbb{Q}[\gamma]$? Is $\mathbb{Z}[\alpha, \beta] = \mathbb{Z}[\gamma]$?

Proof. $\mathbb{Q}[\alpha, \beta] = \mathbb{Q}[\gamma]$. To show this, we need to show that $\mathbb{Q}[\alpha, \beta] \subseteq \mathbb{Q}[\gamma]$ and $\mathbb{Q}[\gamma] \subseteq \mathbb{Q}[\alpha, \beta]$. By definition of a subring, we know that $(\alpha + \beta) \in \mathbb{Q}[\alpha, \beta]$, so we know that $\mathbb{Q}[\gamma] \subseteq \mathbb{Q}[\alpha, \beta]$. Now we need to show that α and β are in $\mathbb{Q}[\gamma]$. Since $\gamma = \alpha + \beta$, we know that $\gamma^3 = 11\alpha + 9\beta$ is also in $\mathbb{Q}[\gamma]$.

$$\begin{aligned} \gamma^3 - 9\gamma &= 2\alpha \\ \frac{1}{2}[\gamma^3 - 9\gamma] &= \alpha \end{aligned}$$

Since $\frac{1}{2}$ is in \mathbb{Q} , we know that α is in $\mathbb{Q}[\gamma]$. A similar argument can be made to show that β is in $\mathbb{Q}[\gamma]$. Since we have shown that α and β are in $\mathbb{Q}[\gamma]$, we know that $\mathbb{Q}[\gamma] \subseteq \mathbb{Q}[\alpha, \beta]$, $\therefore \mathbb{Q}[\alpha, \beta] = \mathbb{Q}[\gamma]$.

$\mathbb{Z}[\alpha, \beta] \neq \mathbb{Z}[\gamma]$, but I don't know how to prove it. My intuition is that the difference between the two coefficients in a $x\alpha + y\beta$ term will never be 1, and we aren't able to use fractions, so we'll never be able to get α or β on its own. □

Problem 11.1.6: Decide whether or not S is a subring of R , when

- (a) S is the set of all rational numbers a/b , where b is not divisible by 2, and $R = \mathbb{Q}$

Proof. S is closed under multiplication because if we multiply $\frac{a}{b} \frac{c}{d}$, we get $\frac{ac}{bd}$, and we know there is no 3 to factor out of the denominator by definition. S is closed under addition because $\frac{a}{b} + \frac{c}{d} = \frac{ad+cb}{bd}$, where again, a 3 cannot be factored out of the denominator. A similar argument can be made for subtraction (since the denominator is the same). S obviously contains 1 ($\frac{1}{1}$), so S is a subring of \mathbb{Q} . \square

- (b) S is the set of functions which are linear combinations with integer coefficients of the functions $1, \cos nt, \sin nt, n \in \mathbb{Z}$ and R is the set of all real valued functions of t .

Proof. S is not a subring of R because it is not closed under multiplication. $\sin(x)\cos(x) = \frac{1}{2}\sin(2x)$. Since you can't write this as a linear combination of the other functions, you know that it is not in R and S is not closed under multiplication. \square

Problem 11.1.7

(a) *Proof.* \square

(b) *Proof.* \square

Problem 11.1.8

Proof. \square

Problem 11.2.2

Proof. \square

Problem 11.3.1

Proof. \square

Problem 11.3.2

Proof. \square

Problem 11.3.3

Proof. \square

Problem 11.3.5

Proof. \square

Problem 11.3.6

Proof. \square

Problem 11.3.7

Proof. ☐

Problem 11.3.8

Proof. ☐

Problem 11.3.9

Proof. ☐

Problem 11.4.1

Proof. ☐

Problem 11.4.2

Proof. ☐

Problem 11.5.1

Proof. ☐

Problem 11.5.2

Proof. ☐

Problem 11.5.3

Proof. ☐

Problem 11.5.6

Proof. ☐

Problem 11.5.7

Proof. ☐

Problem 11.6.2

Proof. ☐

Problem 11.6.2

Proof. ☐

Problem 11.6.8

Proof. ☐

Problem 11.7.1

Proof. ☐

Problem 11.7.2*Proof.***Problem 11.7.5***Proof.***Problem 11.8.1***Proof.***Problem 11.8.2***Proof.***Problem 11.8.4***Proof.***Problem 11.9.1***Proof.***Problem 11.9.2***Proof.***Problem 11.9.3***Proof.***Problem 11.9.4***Proof.***Problem 11.9.5***Proof.***Problem 11.9.6***Proof.***Problem 11.9.9***Proof.***Problem 11.9.10***Proof.***Problem 11.9.11**

Proof.

□

Problem 11.9.12

Proof.

□

Problem 11.9.12

Proof.

□

Problem 11.M.1

Proof.

□

Problem 11.M.2

Proof.

□

Problem 11.M.3

Proof.

□

Problem 11.M.5

Proof.

□

Problem 11.M.6

Proof.

□