Chapter 7

Rings and fields

Def.: A nonempty set A with two operations $*$ and $\circ$ defined on it $(A, *, \circ)$ is called a ring iff

1. $(A, *)$ is an Abelian (commutative) group
2. $(A, \circ)$ is associative
3. In $(A, *, \circ)$ the operation $*$ is distributive in respect to $\circ$, i.e.

$$a \circ (b * c) = (a \circ b) * (a \circ c)$$

Def.: If ring $(A, *, \circ)$ has a neutral element in respect to $\circ$, then it is called a unitary ring.

Def.: A ring $(A, *, \circ)$ is called commutative if the operation $\circ$ is also commutative.

Examples: $(\mathbb{Z}, +, \times)$ is a commutative ring. $(M_{n\times n}, +, \times)$ is a ring (not commutative).

Notation

Given a ring $(A, +, \times)$:

- we call the operations $+$ and $\times$ as addition and multiplication, respectively;
- we denote by 0 the neutral element of $+$;
- we denote by $-a$ the opposite (inverse) element to a for $+$;
- we denote by 1 the neutral element of $\times$;
- we denote $A^* = A\backslash\{0\}$.

Let's consider the common relation of congruences:

$$(\mathbb{Z}/n\mathbb{Z}, +, \times) = (\mathbb{Z}_n, +, \times)$$

We can easily show that it is a commutative unitary ring: 1) Obviously $(\mathbb{Z}_n, +)$ is a commutative group; 2) $(\mathbb{Z}_n, \times)$ is associative and has the neutral element $1 = [1]_n$; 3) It is distributive:

$$[a]_n \times ([b]_n + [c]_n) = [a]_n[b + c]_n = [ab + ac]_n = [a]_n[b]_n + [a]_n[c]_n$$

4) $\times$ is commutative, thus, it is a commutative ring.

If n is not a prime number, then $\exists q, m \in \mathbb{Z}_n \backslash \{[0]\}$ s.t. $q \times m = 0$. In other words we have devisors of zero.

This does not happen in $\mathbb{Z}$, $\mathbb{Z}_p$, $\mathbb{F}[x]$.

In $\mathbb{Z}_n$: $\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} = 0$. This does not happen in $\mathbb{Z}$.

Def.: In a ring $(A, +, \times)$ we shall call divisor of zero from the left any element $a \in A\backslash\{0\}$ for which $\exists b \in A\backslash\{0\}$ s.t. $a \times b = 0$.

Def.: A ring $(A, +, \times)$ that has no divisors of zero is called the integral domain, i.e. the product of any two nonzero elements is also nonzero.

Examples: $(\mathbb{Z}, +, \times)$ and $(\mathbb{Z}_p, +, \times)$ (p is prime) are integral domains.

More complex example: The set of polynomials over a field, $\mathbb{F}[x]$, is an integral domain. Indeed, given:

$$p_n(x) = \sum_{i=0}^{n} a_i x^i, \quad q_m(x) = \sum_{i=0}^{m} b_i x^i, \quad a_n, b_m \neq 0$$

their product:

$$p_n(x) q_m(x) = a_n b_m x^{n+m} + s_{n+m-1}(x) \neq 0$$

Fields

Intuitively, a field is a set A that is a commutative group with respect to two compatible operations: addition and multiplication (except 0).

Def.: Given a commutative unitary ring $(A, +, \times)$ we say that it is a field if 1) $1 \neq 0$ and 2) $\forall a \in A^*$ there exists its inverse in respect to $\times$, i.e. $a^{-1} \times a = 1$.

In other words: $(A, +, \times)$ is a field if $(A, +)$ and $(A^*, \times)$ are commutative groups

Examples: $(\mathbb{R}, +, \times)$, $(\mathbb{Q}, +, \times)$ are fields.

Problem 7.1 Verify if the following sets are rings, commutative, contain 1, integral domains or fields.

(a) The set of positive integers, i.e., $\mathbb{N}\backslash\{0\}$. It is not a ring since $(\mathbb{N}\backslash\{0\}, +)$ is not a group (no 0).

(b) The integers multiples of 7, i.e., $7\mathbb{Z}$.

$(7\mathbb{Z}, +)$ is a commutative group. Indeed $+$ is associative and commutative, there exist a neutral element 0 and the opposite $-a + a = 0$. Then $\times$ is associative, distributive, and commutative. Thus, it is a commutative ring. However, $\times$ has no neutral element 1. It is not a unitary ring, but it is an integral domain.

(c) $A = \{0, 1, -1, i, -i\}$. $(A, +)$ is not a group $(1 + i \notin A)$

(d) $\mathcal{M}_{2\times 3}(\mathbb{R})$ is not a ring since $a \times b$ is not even defined.

(e) $A = \mathcal{M}_{2\times 2}(\mathbb{Z}_3)$.

$(A,+)$ is a commutative group. $(A,\times)$ is associative and has the neutral element $1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. $(A,+,\times)$ is distributive. Thus it is a unitary ring.

It is not commutative (so it is not a field):

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$$

It is not integral domain:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = 0$$

Subrings and Ideals

Def.: Given a ring $(A, +, \times)$ and $S \subseteq A$ then if $(S, +, \times)$ is a ring, it is called a subring of A.

Def.: Given a ring $(A, +, \times)$ and its subring $(I, +, \times)$, then I is called an ideal of A if $\forall s \in I$ and $\forall a \in A$:

$$as \in I, \quad sa \in I$$

Example: $2\mathbb{Z}$ is an ideal of $\mathbb{Z}$. Indeed, $2\mathbb{Z}$ is a ring (without unity) and $\forall a = 2k \in 2\mathbb{Z}$, $\forall b \in \mathbb{Z}$ we have

$$a \times b = b \times a = 2(kb) \in 2\mathbb{Z}$$

Problem 7.2 (a) Prove that $B \subseteq A$ is a subring of A if $\forall b, b' \in B$ we have $b - b' \in B$, $bb' \in B$.

1) $(B, +)$ is a commutative group:
a) $+$ is associative due to A; b) A has 0 and $-a$: $a + 0 = a$, then $a - a = 0$. Now let $a = b$, $b' = b$ then $b - b = 0 \in B$; c) Opposite element: $b = 0$ then $0 - b' = -b' \in B$. Besides, $+$ is well defined.

2) $\times$ is well defined since $b \times b' \in B$; $\times$ is associative and distributive due to A

(b) If $\forall b, b' \in B$ and $\forall a \in A$ we have $b - b' \in B$, $ab \in B$, and $ba \in B$ then B is an ideal of A.

1) B is a subring: let $a = b'$ then $ab = b'b \in B$. Thus, all conditions of (a) are satisfied and B is a subring.

2) By exercise: ab, $ba \in B$. Thus, it is an ideal.

Problem 7.3 (a) Prove that $B = \{0, 2, 4, 6, 8\}$ is a subring of $\mathbb{Z}_{10}$.

Let $b = [2n]_{10}$ and $b' = [2m]_{10}$. Then $b - b' = 2(n - m) \in B$ and $bb' = 2(2nm) \in B$. Thus by P.7.2 it is a subring.

(b) Is it an ideal?
Let $a = [k]_{10} \in \mathbb{Z}_{10}$ then $ab = ba = 2nk \in B$. So it is.

(c) Construct the multiplication table:

$\times$	0	2	4	6	8
0	0	0	0	0	0
2	0	4	8	2	6
4	0	8	6	4	2
6	0	2	4	6	8
8	0	6	2	8	4

Thus, $[6]_{10} = 1$ and the group is commutative and unitary.

(d) Is it a field?

We check the existence of the inverse: $[2] \times [8] = [6]$, $[4] \times [4] = [6]$. Thus all elements in B^* have inverses and B is a field (it is isomorphic to $\mathbb{Z}_5$, which is a field).

Problem 7.5 Prove that if $a \in A$ is nilpotent than it is a divisor of 0.

Since a is nilpotent, then $\exists n > 1$ s.t. $a^n = 0$. We then can write

$$0 = a^n = a \times a^{n-1} = a^{n-1} \times a, \quad a^{n-1} \in A$$

Thus a is a divisor of zero.

Problem 7.6(b) Find nilpotent elements of $\mathbb{Z}_{12}$.

Let's check all elements: $2^2 = 4$, $2^3 = 8$, $2^4 = 4$. Thus, $[2]_{12}$ is not nilpotent, etc. There is only one nilpotent element:

$$[6^2]_{12} = [36]_{12} = [0]_{12}$$

Problem 7.7: Show that $B = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : \; a, b \in \mathbb{R} \right\}$ is a subring with unity of $\mathcal{M}_{n\times n}(\mathbb{R})$.

Using P.7.2: let $c, c' \in B$ then it is trivial to show that $c - c' \in B$ and $c \times c' \in B$.

Let $f: \; B \to \mathbb{C}$ with $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mapsto a + bi$. Prove that f is an isomorphism of rings.

1. It is a homomorphism. Indeed, let $c, c' \in B$, then a) Addition is trivial:

$$f(c + c') = (a + a') + (b + b')i = f(c) + f(c')$$

b) Multiplication:

$$f(cc') = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix} = \begin{pmatrix} aa' - bb' & ab' + ba' \\ -ba' - ab' & aa' - bb' \end{pmatrix} =$$

$$= (aa' - bb') + (ab' + a'b)i = (a + bi)(a' + b'i) = f(c)f(c')$$

c) Unity is trivial:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mapsto 1 + 0i$$

2. f is bijection. Again trivial $\forall c \in B\ \exists!\ z = f(c) \in \mathbb{C}$ and vice versa.

Thus, f is a ring isomorphism. Since $\mathbb{C}$ is a field, we can conclude that B is also a field.

Polynomials

Def.: Let $\mathbb{F}$ be a field. Then we define the set of polynomials over this field:

$$\mathbb{F}[x] = \{a_0 + a_1 x + \cdots + a_n x^n : \; n \in \mathbb{N}, \; a_i \in \mathbb{F}, \; i = 0, \ldots, n\}$$

Def.: Given $p(x) = a_0 + a_1 x + \cdots + a_n x^n$, $a_n \neq 0$, we shall call the polynomial degree: $\deg(p) = n$.

Def.: Given two polynomial $p(x)$ and $q(x)$ of degrees n and m, respectively. Assuming $n \leq m$ we define:

1. Addition of polynomial as:

$$s(x) = p(x) + q(x) = \sum_{k=0}^{m} c_k x^k, \quad c_k = a_k + b_k$$

Note: for $p(x)$ we set $a_k = 0$ for $k > n$.

2. Product of polynomial as:

$$r(x) = p(x)q(x) = \sum_{k=0}^{n+m} c_k x^k, \quad c_k = \sum_{i=0}^{k} a_i b_{k-i}$$

Note that: $\deg(s) \leq m$, $\deg(r) = n + m$.

Similar to integers we can state the remainder theorem for polynomials.

Theorem: (about remainder) Let $\mathbb{F}[x]$ be a ring of polynomials defined over a field $\mathbb{F}$. Then for all $P, Q \in \mathbb{F}[x]$ $(Q \neq 0)$ $\exists! s, r \in \mathbb{F}[x]$ s.t.

$$P(x) = s(x)Q(x) + r(x), \quad \deg(r) < \deg(Q)$$

Problem 7.8: Divide polynomials:
(a) $P(x) = x^4 + 3x^3 + 2x^2 + x + 4$, $Q(x) = 3x^2 + 2x$ in $\mathbb{Z}_5[x]$.

We need $[3]_5^{-1} = [2]_5$. Then, e.g. $1 = 2 \times 3$, $4 \times 2 = 3$, etc.

$$\begin{array}{rl}
x^4+3x^3+2x^2+x+4 & \underline{\left|\,3x^2+2x\right.} \\
-\underline{x^4+4x^3} & 2x^2+3x+2 \\
4x^3+2x^2+x+4 & \\
\underline{4x^3+x^2} & \\
x^2+x+4 & \\
-\underline{x^2+4x} & \\
2x+4 &
\end{array}$$

Thus,

$$P = (2x^2 + 3x + 2)Q(x) + 2x + 4$$

(b) $P(x) = x^{10}$, $Q(x) = x^2 + 1$ in $\mathbb{Z}_2[x]$.
Note that $-1 = 1$ in $\mathbb{Z}_2$

Thus

$$x^{10} = (x^8 + x^6 + x^4 + x^2 + 1) \times (x^2 + 1) + 1$$

Let $\mathbb{F}$ be a field and $P, Q \in \mathbb{F}[x]$ $(Q \neq 0)$. Then:

Def.: We say that Q divides P if there exists $q \in \mathbb{F}[x]$ s.t.

$$P(x) = q(x)Q(x)$$

Def.: We say that $P(x)$ is irreducible if any polynomial Q that divides P has either $\deg(Q) = 0$ or $\deg(Q) = \deg(P)$.

Def.: We say that $D \in \mathbb{F}[x]$ is the greatest common divisor of P and Q if $D|P$ and $D|Q$. Besides, if $h|P$ and $h|Q$, then $\deg(h) \leq \deg(D)$.

Lemma of Bezout. Given $P, Q \in \mathbb{F}[x]$ and $D = \gcd(P, Q)$. Then there exist $u, v \in \mathbb{F}[x]$ s.t.

$$D(x) = u(x)P(x) + v(x)Q(x)$$

Euclides algorithm

Let $P, Q \in \mathbb{F}[x]$ and $P(x) = q(x)Q(x) + r(x)$ $(\deg(r) < \deg(Q))$.
Then we construct the table:

r_i	P	Q	r
q_i		q	
α_i	1	0	
β_i	0	1	

where r_i, α_i, and β_i are calculate by:

$$r_i = r_{i-2} - q_{i-1} r_{i-1}$$

Then

$$r_n(x) = \gcd(P, Q) = \alpha_n(x)P(x) + \beta_n(x)Q(x)$$

Problem 7.10: Find the greatest common divisor of the following polynomials and write them in the form $a(x)f(x) + b(x)g(x)$:

(a) $f(x) = x^3 - 1$, $g(x) = x^4 - x^3 + x^2 + x - 2$ in $\mathbb{Q}[x]$

g	f	$x^2 + 2x - 3$	$7x - 7$	0
	$x - 1$	$x - 2$	$\frac{1}{7}x + \frac{3}{7}$	
1	0	1	$-x + 2$	
0	1	$-x + 1$	$1 + (x-1)(x-2)$	

$g = (x-1)f + x^2 + 2x - 3$; $f = (x-2)(x^2 + 2x - 3) + 7x - 7$; $x^2 + 2x - 3 = \left(\frac{1}{7}x + \frac{3}{7}\right)(7x - 7)$. Thus

$$7x - 7 = (-x + 2)(x^4 - x^3 + x^2 + x - 2) + (x^2 - 3x + 3)(x^3 - 1)$$

Problem 7.11 Find zeros

(a) $f(x) = x^5 + 3x^3 + x^2 + 2x \in \mathbb{Z}_5[x]$

$$f(x) = x(x^4 + 3x^2 + x + 2)$$

Thus, $x = 0$ is a root. Now assume $x \neq 0$ and by using Fermat ($a^4 = 1$ in $\mathbb{Z}_5$) we get that roots can be found from $3x^2 + x + 3 = 0 = (x - \alpha)(3x + c) = 3(x - \alpha)(x - 3c)$. Then $3\alpha c = 1 \;\Rightarrow\; 3c = \alpha^{-1}$. Thus, $3x^2 + x + 3 = 3(x - \alpha)(x - \alpha^{-1})$.

$$\begin{aligned} \alpha = 1 \quad &\Rightarrow \quad 3 + 1 + 3 = 2 \neq 0 \\ \alpha = 2 \quad &\Rightarrow \quad 12 + 2 + 3 = 2 \neq 0 \\ \alpha = 3 = -2 \quad &\Rightarrow \quad 12 - 2 + 3 = 3 \neq 0 \\ \alpha = 4 = -1 \quad &\Rightarrow \quad 3 - 1 + 3 = 0 \end{aligned}$$

Thus, $\alpha = 4$ and $\alpha^{-1} = 4^{-1} = 4$ are roots (i.e. 4 is a double root).

(b) $g = x^5 - x \in \mathbb{Z}_5[x]$.

$$g = x(x^4 - 1)$$

We know that $x - 1 | x^n - 1$ (Ex. 9). Thus by dividing:

$$x^4 - 1 = (x^3 + x^2 + x + 1)(x - 1)$$

Therefore $g = x(x-1)(x^3 + x^2 + x + 1)$. Then we can check that $x = 1$ is not multiple. For $x = 2$ we have $3 + 4 + 2 + 1 = 0$. Then $g = x(x-1)(x-2)(x^2 + 3x + 2)$. We now see $x = -1$ is also a root. Finally:

$$g = x(x-1)(x-2)(x-3)(x-4).$$

From the other side: $x^4 - 1 = 1 - 1 = 0$ $(x \neq 0)$. Thus, for any x we $g(x) = 0$, which means that $x = 0, 1, 2, 3, 4$ are roots and we get the same result.

Multiple roots

If α is a root of $p \in \mathbb{F}[x]$ then

$$p(x) = (x - \alpha)q(x)$$

If $\alpha \in \mathbb{F}$ then $q \in \mathbb{F}[x]$ (if not then q belongs to a bigger set).

If $\deg(p) = n$ then p at most has n roots.

Def.: We say that α is a root of $p \in \mathbb{F}[x]$ of multiplicity k if

$$p(x) = (x - \alpha)^k q(x), \quad q \in \mathbb{F}[x], \; q(\alpha) \neq 0$$

Def.: Given $p \in \mathbb{F}[x]$ of degree n we introduce its derivative as:

$$p'(x) = a_1 + 2a_2 x + 3a_3 x^2 + \cdots + n a_n x^{n-1}$$

Example: [P.7.12(c)] $p = x^3 + x + 1$ in $\mathbb{Z}_3[x]$:

$$p' = [3]_3 x^2 + [1]_3 = 1$$

If $p' = 0$ then all roots of p are multiple. Indeed, Let α be a root of p, then

$$p = (x-\alpha)q \;\Rightarrow\; p' = q + (x-\alpha)q' = 0 \;\Rightarrow\; p = (x-\alpha)^2(-q)$$

Theorem: Let $p \in \mathbb{F}[x]$ such that $p' \neq 0$. Then the next statements are equivalent: a) There exists a multiple root α; b) $(x-\alpha)$ divides p and p'; c) $h = \gcd(p, p')$ s.t. $\deg(h) = n \geq 1$ and $a_n = 1$.

Searching for multiple roots

Let $\alpha \in \mathbb{F}$ be a multiple root of $p \in \mathbb{F}[x]$. Then

$$p(x) = (x-\alpha)^k q(x), \quad q \in \mathbb{F}[x], \quad q(\alpha) \neq 0$$

The derivative:

$$p'(x) = k(x-\alpha)^{k-1}q(x)+(x-\alpha)^k q'(x) = (x-\alpha)^{k-1}[kq(x)+(x-\alpha)q'(x)]$$

Denoting $h = kq(x) + (x-\alpha)q'(x)$ we observe:

$$p'(x) = (x-\alpha)^{k-1}h(x), \quad h \in \mathbb{F}[x], \quad h(\alpha) = kq(\alpha) \neq 0$$

Thus,

$$(x-\alpha)^{k-1}|p(x) \;\text{ and }\; (x-\alpha)^{k-1}|p'(x)$$

We thus have to find the $\gcd(p, p')$. If it can be presented in the form $c(x-\alpha)^n$, then α is a root of multiplicity $n+1$.

Problem 7.12 Which polynomials have multiple roots?

(a) This is horrible. Don't continue.

(b) $g(x) = x^3 + 2x - i$ in $\mathbb{C}[x]$

$$g'(x) = 3x^2 + 2$$

Let's find the gcd by the Euclides algorithm:

g	g'	$\frac{4}{3}x - i$	$\frac{5}{16}$	0
	$\frac{x}{3}$	$\frac{9}{4}x + \frac{27}{16}i$	$\frac{64}{15}x - \frac{16}{5}i$	

Thus $\gcd(g, g') = \frac{5}{16} \Rightarrow \deg(\gcd(g, g')) = 0$ and hence there are no multiple roots.

(c) $f = x^3 + x + 1$ in $\mathbb{Z}_3[x]$

$$f' = 3x^2 + 1 = 1 \quad \Rightarrow \quad \gcd(f, f') = 1 \quad \Rightarrow \quad \deg(1) = 0$$

Thus, f has no multiple roots.

(g) $f = x^5 + 5x^4 + 3x^3 + 2x + 1$ in $\mathbb{Z}_7[x]$

$$f' = 5x^4 - x^3 + 2x^2 + 2$$

Let's find gcd

f	f'	$x^2 + 3x + 2$	$3x + 6$	0
	$3(x+1)$	$5(x^2 + x + 1)$	$5(x+1)$	

Thus, $\gcd(f, f') = 3x + 6$, $\deg(3x + 6) = 1$ and therefore there are multiple roots. Namely:

$$3x + 6 = 3(x + 2) = 3(x - 5)$$

Thus, $x = 5$ is a root with multiplicity 2.