AFCS/Spring 2014

Rings and Fields

Prof.Dr. Ferucio Laurenţiu Ţiplea

"Al. I. Cuza" University of Iaşi Department of Computer Science Iasi 740083, Romania

E-mail: fltiplea@mail.dntis.ro

URL: http://www.infoiasi.ro/~fltiplea

Contents

- 1. Definitions and examples
- 2. Ring homomorphisms
- 3. Characteristic of a ring
- 4. Finite fields
- 5. Applications to cryptography

Definition 1 A ring is an algebraic structure $(R, +, -, 0, \cdot)$ such that:

- ullet (R,+,-,0) is commutative group;
- lacksquare (R,\cdot) is a semigroup;
- is left- and right-distributive over +.

Remark 1 Let $(R, +, -, 0, \cdot)$ be a ring.

- 1. 0 is called the zero element of R; it is unique;
- 2. If · is commutative then the ring is called **commutative**;
- 3. We will usually denote rings just by their carrier sets. That is, we will often say "Let R be a ring".

Proposition 1 Let $(R, +, -, 0, \cdot)$ be a ring. Then:

- (1) a0 = 0a = 0, for any $a \in R$;
- (2) (-a)b = a(-b) = -(ab), for any $a, b \in R$;
- (3) (-a)(-b) = ab, for any $a, b \in R$;
- (4) a(b-c)=ab-ac and (b-c)a=ba-ca, for any $a,b,c\in R$;
- (5) $(\sum_{i=1}^{n} a_i)(\sum_{j=1}^{m} b_j) = \sum_{i=1}^{n} \sum_{j=1}^{m} a_i b_j$, for any $n, m \ge 1$ and $a_i, b_j \in R$, $1 \le i \le n$, and $1 \le j \le m$.

Proposition 2 Let R be a ring. Then:

(1)
$$(-m)a = -(ma);$$

(2)
$$(m+n)a = ma + na$$
;

(3)
$$m(a+b) = ma + mb$$
;

(4)
$$(mn)a = m(na);$$

(5)
$$m(ab) = (ma)b = a(mb);$$

(6)
$$(ma)(nb) = (mn)(ab),$$

for any $a, b \in R$ and $m, n \ge 1$.

Proposition 3 Let R be a commutative ring. Then,

$$(a+b)^n = \sum_{k=0}^n C_n^k a^{n-k} b^k,$$

for any $a,b \in R$ and $n \ge 1$, where $C_n^k = n!/(k!(n-k)!)$, for any $0 \le k \le n$.

Proof By mathematical induction on $n \geq 1$. \square

Definition 2 A ring with unity/identity is an algebraic structure $(R, +, -, 0, \cdot, e)$ which satisfies:

- \blacksquare (R,+,-,0) is a commutative group;
- lacksquare (R,\cdot,e) is a monoid;
- is left- and right-distributive over +.

The element e, also denoted by 1_R or 1, is called the unity/identity of R.

Proposition 4 If $(R, +, -, 0, \cdot, e)$ is a ring with unity then e = 0 iff $R = \{0\}$.

A ring with unity $(R, +, -, 0, \cdot, e)$ which satisfies e = 0 is called a trivial/null ring.

Definition 3

- (1) A division ring is an algebraic structure $(R, +, -, 0, \cdot, ', e)$ which satisfies:
 - (R, +, -, 0) is a commutative group;
 - (R, \cdot, e) is a monoid and $e \neq 0$;
 - ' is a unary operation which satisfies aa' = a'a = e, for any $a \neq 0$;
 - is left- and right-distributive over +.
- (2) A commutative division ring is called a field.

Definition 4

- (1) An element $a \in R \{0\}$ of a ring R is called a zero divisor if there exists $b \in R \{0\}$ such that ab = 0 or ba = 0.
- (2) A commutative ring R with unity $e \neq 0$ and with no zero divisors is called an integral domain.

Proposition 5

- 1. If R is a ring and $c \in R \{0\}$ is not a zero divisor, then ac = bc (ca = cb) implies a = b, for any $a, b \in R$.
- 2. Division rings do not have zero divisors.
- 3. Any field is an integral domain.
- 4. Any finite integral domain is a field.
- 5. Let $p \geq 2$. \mathbb{Z}_p is a field iff p is a prime.

Example 1

- (1) Let (R,+,-,0) be a commutative group. Define on R the binary operation \cdot by $a\cdot b=0$, for any $a,b\in R$. Then, $(R,+,-,0,\cdot)$ is a ring.
- (2) **Z**, together with addition and multiplication, form an integral domain, but not a field.
- (3) Q, R, and C, together with addition and multiplication, form fields.
- (4) $n\mathbf{Z}$ is a commutative ring with no zero divisors. This ring has unity only if n=-1, n=0, or n=1 (for n=0, the ring is null).
- (5) \mathbf{Z}_n is a commutative ring with unity. If n is a prime, then \mathbf{Z}_n is a field.

2. Ring homomorphisms

Definition 5 Let R_1 and R_2 be rings. A function $h:R_1\to R_2$ is a ring homomorphism if

- b(ab) = h(a)h(b),

for any $a, b \in R_1$

The second property in the definition above may only be required for $a, b \in R_1 - \{0\}$. Indeed, if, for instance, b = 0, then

$$h(a0) = h(0) = 0 = h(a)0 = h(a)h(0).$$

If R_1 and R_2 have units e_1 and e_2 , then the property

$$h(e_1) = e_2$$

is required too.

3. Characteristic of a ring

Definition 6 We say that a ring R has characteristic $n \ge 1$, if n is the smallest natural number such that na = 0, for any $a \in R$ (if there is such a number n).

If does not exist $n \ge 1$ with na = 0 for any $a \in R$, then we say that R has characteristic zero.

The characteristic of a ring R will be denoted by char(R).

Remark 2 A ring with unity $e \neq 0$ cannot have the characteristic 1. Therefore, the only ring of characteristic 1 is the null ring.

3. Characteristic of a ring

Example 2

- (1) \mathbf{Z}_m has characteristic m, for any $m \geq 1$.
- (2) Z is an integral domain of characteristic zero.
- (3) Q, R, and C are fields of characteristic zero.

3. Characteristic of a ring

Theorem 1 Let $(R,+,-,0,\cdot,e)$ be a ring with unity of characteristic $n\geq 1$.

- (1) n is the smallest non-zero natural number which satisfies ne = 0.
- (2) If $e \neq 0$ and R does not have zero divisors, then n is a prime.
- (3) If the characteristic of an integral domain is not zero, then it is a prime.
- (4) The characteristic of a finite field is a prime number.

Theorem 2 If R is a finite field of characteristic p, then $|R| = p^n$, for some $n \ge 1$.

Theorem 3 For any prime p and $n \ge 1$, there exists a field with p^n elements.

Theorem 4 Any two finite fields with the same number of elements are isomorphic.

The finite field with p^n elements, which is unique up to isomorphism, is denoted by $GF(p^n)$ or F_{p^n} and it is called the Galois field with p^n elements.

Theorem 5 Any subfield of a field $GF(p^n)$ is of the form $GF(p^m)$, where m|n, and vice versa.

Constructing $GF(p^n) - p$ is a prime and $n \ge 1$

- **•** let f be a polynomial of degree n with coefficients in \mathbb{Z}_p ;
- the set F of all polynomials over \mathbb{Z}_p of degree at most n-1 has exactly p^n elements;
- If f is irreducible over $\mathbf{Z}_p[x]$, then F together with the following operations form a field:
 - the addition of two polynomial in F is the component-wise addition modulo p;
 - the multiplication of two polynomials in F is performed modulo p for coefficients and modulo f for the entire result;
 - the zero element is the zero polynomial, and the unity of F is the constant polynomial 1;
 - the additive (multiplicative) inverse exists for any polynomial (non-zero polynomial) in F.

Constructing $GF(p^n)$ – Example

- ullet we want to construct $GF(2^8)$;
- let $f(x) = x^8 + x^4 + x^3 + x + 1 \in \mathbb{Z}_2[x]$ be an irreducible polynomial of degree 8 over $\mathbb{Z}_2[x]$;
- $GF(2^8)$ consists of all polynomial of degree at most 7 with coefficients in $\mathbb{Z}_2 = \{0, 1\}$;
- example of addition in $GF(2^8)$:

$$(x^6 + x^4 + x^2 + x + 1) + (x^7 + x + 1) = x^7 + x^6 + x^4 + x^2$$

• example of multiplication in $GF(2^8)$:

$$(x^6 + x^4 + x^2 + x + 1)(x^7 + x + 1) = x^7 + x^6 + 1$$

Irreducible polynomials – Example

- $f(x) = x^2 + x + 1$ is irreducible over $\mathbb{Z}_2[x]$. This polynomial can be used to define $GF(2^2)$;
- $f(x) = x^3 + x^2 + x + 2$ is irreducible over $\mathbb{Z}_3[x]$. This polynomial can be used to define $GF(3^3)$;
- $f(x) = x^8 + x^4 + x^3 + x + 1 \in \mathbf{Z}_2[x]$ is irreducible over $\mathbf{Z}_2[x]$. This polynomial is used by the cryptosystem Rijndael (AES) to define $GF(2^8)$.