KTH Teknikvetenskap

SF2729 GROUPS AND RINGS
LECTURE NOTES
2010-03-23

SANDRA DI ROCCO

CONTENTS

1. RINGS-FIELDS AND INTEGRAL DOMAINS

1.1. **Rings and Fields.** This is the first lecture of the second part of the course. We start by "expanding" the structure of an abelian group in order to define reacher algebraic structures.

Definition 1.1. A *ring* $(R, +, \cdot)$ is a set R with two binary operations:

$$+ : R \times R \to R, \cdot : R \times R \to R,$$

such that

(1) $(R, +)$ is an abelian group.
(2) $\cdot$ is associative, i.e. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$.
(3) For all $a, b, c \in R$, it is $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$

Example 1.2. (1) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are rings (notice commutative!).
(2) Observe that $0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$ which implies that $0 \cdot a = a \cdot 0 = 0$ for all $a \in R$. Any ring with unity where $0 = 1$ consists of $R = \{0\}$ and it is called the trivial ring.

(3) If R_1, R_2 are rings then $R_1 \times R_2$ can be given the structure of a ring, using coordinatewise operations.
(4) Let R be a ring and X be a set. The set of functions from X to R usually denoted by R^X cen be given the structure of a ring, using he operations on R.
(5) (Gaussian integers) $\mathbb{Z}[i] = \{a + bi, a, b \in \mathbb{Z}\}$ with

$$(a + bi) + (c + di) = (a + c) + (b + d)i, (a + bi) \cdot (c + di) = (ac - bd) + (ad + cb)i.$$

Definition 1.3. Let R be a ring, if in addition there is an element (multiplicative unit) 1 such that $1 \cdot a = a \cdot 1 = a$ for all $a \in R$ then the ring is said to be a *ring with unit.*

If the multiplication is commutative, i.e. $a \cdot b = b \cdot a$ for all $a, b \in R$, then the ring is said to be a *commutative ring*.

An element x such that $x \cdot a = 1$ is called a *multiplicative inverse* of a and it is denoted by a^{-1}, (if there is one it is unique!). If an inverse exists the element is called invertible (or sometimes a unit).

If every non zero element in a ring R with a unity has an inverse the ring is called a *division ring*.

A commutative division ring is called a *field.*

Example 1.4.
- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields.
- $\mathbb{Z}_n$ is a commutatine ring. When is it a Field?

Let $(R, +, \cdot)$ be a ring, by R^* we denote the set of invertible elements in R. (what is $\mathbb{Z}[i]^*$?).

Proposition 1.5. *Let $(R, +, \cdot)$ be a ring with unity 1, then $(R^*, \cdot)$ is a group.*

Proof. Let $a, b \in R^*$, the associativity property gives that:

$$(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = 1, (b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = 1,$$

which implies that $a \cdot b \in R^*$. □

A consequence of this is the so called *Little theorem of Fermat* that we will see later.

1.2. **Integral Domains.**

Definition 1.6. Lat R be a ring. Elements $0 \neq a, b \in R$ are said to be a zero-divisors if $a \cdot b = 0$.

Example 1.7. In $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ there are no zero-divisors, but in $\mathbb{Z}_6$ there are, ex $[3] \cdot [2] = [0]$.

Proposition 1.8. *The element $0 \neq [m] \in \mathbb{Z}_n$ is a zero-divisor if and only if $gcd(m, n) \neq 1$.*

Proof. Assume that $gcd(m, n) = d \neq 1$ then $[\frac{n}{d}] \neq 0$ and $[m] \cdot [\frac{n}{d}] = [n][\frac{m}{d}] = 0$. Assume now that there is an $0 \neq [s] \in \mathbb{Z}_n$ such that $[s] \cdot [m] = 0$ then it is $ms = kn$ for some $k \in \mathbb{Z}$. If $gcd(m, n) = 1$ then n should divide s and thus $[s] = 0$, which implies that $gcd(m, n) \neq 1$. □

A corollary of the previous proposition is that $\mathbb{Z}_p$ is a field only if p is prime.

Theorem 1.9 (Little theorem of Fermat)**.** *If $a \in \mathbb{Z}$ and p is a prime not dividing a then p divides $a^{p-1} - 1$.*

Proof. $(\mathbb{Z}_p^*, \cdot)$ is a group of order $p-1$. it follows that the (multiplicative) order of every element devides $p-1$. It follows that if $a \neq 0 \mod p$ then $[a^{p-1}] = [1]$ which means that p divides $a^{p-1} - 1$. □

One can easily generalize this theorem and prove the so called *Euler's theorem*. Define the Euler number:

$$\phi(n) = \{0 < k \leq n, s.t. gcd(k, n) = 1\}.$$

We will see that $\phi(n)$ is exactly the cardinality of the group $(\mathbb{Z}_n^*, \cdot)$, i.e. all non zero divisors are invertible. Then a similar prove gives:

Theorem 1.10. *If $a \in \mathbb{Z}$ is relatively prime to n, then n divides $a^{\phi(n)} - 1$.*

The *camcellation law* in a ring R is the following:

$$a \neq 0, a \cdot b = a \cdot c \Rightarrow b = c.$$

Proposition 1.11 (Cancellation law)**.** *The cancellation laws hold in a ring R if and only if it has no zero-divisors.*

Proof. Assume that the cancellation laws hold and let a, b zero divisors, then $a \cdot b = 0 = a \cdot 0$ would implie $b = 0$, which is a contradiction. Assume there are no zero-divisors and let $a \neq 0, a \cdot b = a \cdot c$, then $a \cdot b - a \cdot c = a \cdot (b - c) = 0$ which must implie $b - c = 0$ and thus $b = c$. □

Observe that the unity 1 in a ring cannot be a zero-divisor (prove it). This implies that division rings have no zero-divisors. More generally all subrings of division rings have no zero- divisors.

Example 1.12 (thm 20.5 i the book)**.** Let $m \in \mathbb{Z}, m > 0$, let $[a], [b] \in \mathbb{Z}_m$ and let $d = gcd(a, m)$.

(1) $ax \equiv_m b$ has a solution $\Leftrightarrow d \backslash b$.
(2) If $d \backslash b$ the equation has exactly d solutions.

Assume that $ax \equiv_m b$ has a solution s. That means that $as - b = km$ for some $k \in \mathbb{Z}$ and thus $d \backslash b$ because $d \backslash a, m$. Assume that $d \backslash b$ and write $b = db_1, a = da_1, m = dm_1$ we see that $[s] \in \mathbb{Z}_n$ is a solution of $ax \equiv_m b$ if and only if s_1 is a solution of $a_1 x \equiv_{m_1} b_1$. Because $gcd(a_1, m_1) = 1$ $[a_1]$ is invertible in $\mathbb{Z}_{m_1}$ and thus $a_1 x \equiv_{m_1} b_1$ does have a unique solution. The numbers $s_1, s_1 + m_1, \ldots, (d-1)m_1$ all reduce to s_1 modulo m_1 and therrfore are solution of the original modular equation.

Definition 1.13. A non trivial commutative ring with no zero-divisors is called an *integral domain*.

Definition 1.14. A subset $S \subset R$, of a ring $(R, +, \cdot)$ is a *subring* if $(S, +, \cdot)$ is a ring. In other words one has to check that :

$$0 \in S, (S, +) \text{ is a group }, a \cdot b \in S \text{ for all } a, b \in S.$$

Example 1.15. $\mathbb{C}$ is an integral domain, $\mathbb{Z}[i] \subset \mathbb{C}$ is a subring and therefore it is an integral domain.

1.3. **Ring-homorphisms.**

Definition 1.16. Let R_1, R_2 be two rings. A function $f : R_1 \to R_2$ is said to be a *ring homomorphism* if:

(1) $f(a+b) = f(a) + f(b)$,
(2) $f(a \cdot b) = f(a) \cdot f(b)$.

and if it is bijective it is called an *ring-isomorhism* and we write $R_1 \cong R_2$...

If $R_1 = R_2$ ia ring-homomorphism is called an *endmorphism* and if it is bijective it is called an *automorphism*

Example 1.17.
- $f : \mathbb{Z} \to \mathbb{Z}_n$ is a ring homorphism.
- the inclusion $S \to R$ is a ring-homomorphism for any subring $S \subset R$.
- the projections $\pi_i : R_1 \times R_2 \to R_i$ are ring-homorphisms for $i = 1, 2$.
- For any r, s such that $gcd(r, s) = 1$, it is $\mathbb{Z}_{rs} \cong \mathbb{Z}_r \times \mathbb{Z}_s$, via the map $f(n \cdot 1_{\mathbb{Z}_{rs}}) = n \cdot (1, 1)$.

1.4. **Characteristics.**

Definition 1.18. The smallest integer $r \in \mathbb{Z}$ such that $r \cdot a = 0$ for all element a is a ring R is called the *characteristic* of the ring R. If such an integer does not exist, the ring R is said to have characteristics 0.

Example 1.19.
- The characteristic of $\mathbb{Z}_n$ is n, while $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ have characteristic zero.
- Observe that if R is a ring with unity, 1, then the characteristic is the smallest r such that $r \cdot 1 = 0$.
- Observe that The characteristic of any non trivial field F is either 0 or a prime number. The distributive property gives that:

$$nm1 = n1 \cdot m1.$$

RECOMMENDED EXCERCISES

IV-18 Rings and Fields. 7-12, 14-19, 23-25, 38,44,46,49.

IV-19 Integral Domains. 14,26,30

IV-20 Fermat's Theorem. 8,9,27-30.