Some slides for 1st Lecture, Algebra 2

Diego Ruano

Department of Mathematical Sciences
Aalborg University
Denmark

5-02-2014

A ring (ring) is an abelian group $(R, +)$ (the neutral element is 0) with an additional composition $\cdot$ called multiplicaton with satifies (for every $x, y, z \in R$:

1. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
2. There exists an element $1 \in R$ s.t. $1 \cdot x = x \cdot 1 = x$
3. $x \cdot (y + z) = x \cdot y + x \cdot z$ and $(y + z) \cdot x = y \cdot x + z \cdot x$.

A subset $S \subset R$ of a ring is called a subring (delring) if S is a subgroup of $(R, +)$, $1 \in S$ and $xy \in S$ for $x, y \in S$.

An element $x \in R \setminus \{0\}$ is called a zero divisor (nuldivisor) if there exists $y \in R \setminus \{0\}$ s.t. $xy = 0$ or $yx = 0$.

A ring (delring) is an abelian group $(R, +)$ (the neutral element is 0) with an additional composition $\cdot$ called multiplicaton with satifies (for every $x, y, z \in R$:

1. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
2. There exists an element $1 \in R$ s.t. $1 \cdot x = x \cdot 1 = x$
3. $x \cdot (y + z) = x \cdot y + x \cdot z$ and $(y + z) \cdot x = y \cdot x + z \cdot x$.

R is called commutative (kommutativ) if $xy = yx$ for every $x, y \in R$.

An element $x \in R$ is called a unit (enhed) if there exists $y \in R$ s.t. $xy = yx = 1$. In this case we say $x^{-1} = y$ is the inverse of x. The set of units in R is denoted R^*.

Exercise: $(R^*, \cdot)$ is a group. R^* is abelian if R is commutative

Exercise: If $R \neq \{0\}$, then $0 \notin R^*$

examples

Two non-commutative ring

- The 2×2-matrices
- Quaternions (Kvaternioner):

$$\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{C}\}$$

$\cdot$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

However, we will work here only with commutative rings. So a ring will be always commutative for us without any further notice.

A ring R with $R^* = R \setminus \{0\}$ is called a field (legeme).

If $K \subset L$ are fields and K is a subring of L then K is called a subfield (dellegeme)of L and L is called an extension field (udvidelseslegeme) of K.

A domain (område) is a ring $R \neq \{0\}$ with no zero divisors.

Proposition 3.1.3

Let R be a domain and $a, x, y \in R$. If $a \neq 0$ and $ax = ay$ then $x = y$

Proof:

- $ax = ay \Rightarrow ax - ay = 0 \Rightarrow a(x - y) = 0$
- Wrong!!!: Multiply by a^{-1}, to get $x - y = 0 \Rightarrow x = y$.
- Since $a(x - y) = 0$, $a \neq 0$ and R is domain, we have that $x - y = 0$, to get $x = y$.

Proposition 3.1.4

let F be a field. Then F is a domain.

Proof:

- Suppose $x, y \in F$, $x \neq 0$ and $xy = 0$. Is $y = 0$???
- Since $x \neq 0$, there exists x^{-1}.
- Hence, $0 = x^{-1}0 = x^{-1}(xy) = y$

Examples

- $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\} \subset \mathbb{C}$
- $(a + bi) + (c + di) = (a + c) + (b + d)i$
- $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$
- For $z = a + bi \neq 0$:

$$\frac{1}{z} = \frac{a - bi}{(a + bi)(a - bi)} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} i$$

- $N(z) = |z|^2 = z\bar{z} = a^2 + b^2$.
- One has that $N(z_1 z_2) = N(z_1)N(z_2)$
- $\mathbb{Q}(i)$ is an extension field of $\mathbb{Q}$ and a subfield of $\mathbb{C}$

Gaussian integers (Gaussiske heltal):
$\mathbb{Z}(i) = \{a + bi : a, b \in \mathbb{Z}\}$

Lemma

$z \in \mathbb{Z}[i]$ is a unit if and only if $N(z) = 1$. One has that

$$\mathbb{Z}[i]^* = \{1, -1, i, -i\}$$

Proof $\Rightarrow$):

- If z is a unit then $1 = N(1) = N(zz^{-1}) = N(z)N(z^{-1})$
- Since $N(z)$ and $N(z^{-1}) \in \mathbb{N}$, then $N(z) = 1$

Proof $\Leftarrow$):

- $z = a + bi$ with $N(z) = (a + bi)(a - bi) = a^2 + b^2 = 1$
- Then $zy = 1$ for $y = a - bi \in \mathbb{Z}[i]$.

An ideal (ideal) in a ring R is a subgroup I of $(R, +)$ such that $\lambda x \in I$ for every $\lambda \in R$ and $x \in I$

R is an ideal.
Exercise 3.4: Let $I \subset R$, $I = R \Leftrightarrow 1 \in I$

An equivalent definition of ideal: An ideal I of R is a subset $I \subset R$ such that:

1. $0 \in I$
2. If $x, y \in I$, then $x + y \in I$
3. If $x \in I$ and $\lambda \in R$, then $x\lambda \in I$.

Let $r_1, \ldots r_n \in R$, then

$$\langle r_1, \ldots, r_n \rangle = \{\lambda_1 r_1 + \cdots + \lambda_n r_n : \lambda_1, \ldots, \lambda_n \in R\}$$

is an ideal in R (exercise 3.5).

Let $r_1, \ldots r_n \in R$, then

$$\langle r_1, \ldots, r_n \rangle = \{\lambda_1 r_1 + \cdots + \lambda_n r_n : \lambda_1, \ldots, \lambda_n \in R\}$$

is an ideal in R (exercise 3.5).

If I is an ideal in R and there exist $r_1, \ldots, r_n \in R$ such that $I = \langle r_1, \ldots, r_n \rangle$, we say that I is finitely generated (endeligt frembragt ideal) by $r_1, \ldots, r_n \in R$.

An ideal generated by infinitely many elements?:

Let $M \subset R$, the ideal generated by M is: $\langle f : f \in M \rangle =$

$$\{a_1 f_1 + \cdots + a_n f_n : n \in \mathbb{N}, a_1, \ldots a_n \in R, f_1 \ldots, f_n \in M\}$$

Remark 3.1.8

Let I, J be ideals in ring R

1. Then $I \cap J$ and $I + J = \{i + j : i \in I, j \in J\}$ are also ideals in R
2. The product IJ is defined to be the ideal generated by $\{ij : i \in I, j \in J\}$. We have $IJ \subset I \cap J$.

Exercise: in a field F the only ideals are $\{0\}$ and F.

An ideal I in R that can be generated by one element is called a principal ideal (hovedideal) (that is, there exists $d \in R$ s.t. $I = \langle d \rangle$.

A domain in which every ideal is a principal ideal is called a principal ideal domain (hovedidealområde).

Proposition 3.1.10

The ring $\mathbb{Z}$ is a principal ideal domain.

Theorem 3.1.11

The ring of Gaussian integers $\mathbb{Z}[i]$ is a principal ideal domain.

Proof: $I \subset \langle d \rangle$ (the converse is trivial)

- Let I be anon-zero ideal in $\mathbb{Z}[i]$. Choose $d = a + bi \in I$, $d \neq 0$, such that $N(d) = a^2 + b^2$ is minimal.
- Suppose that $z \in I$, then $z/d = p_1 + p_2 i \in \mathbb{C}$, with $p_1, p_2 \in \mathbb{Q}$.
- Note: Any element of $\mathbb{C}$ is at distance at most $\sqrt{2}/2$ to a point with integer real and imaginary parts (think in the lattice).
- So, consider $q \in \mathbb{Z}[i]$ s.t. $|z/d - q| < 1$ (or $N(z/d - q) < 1$
- Multiply by $N(d)$: $N(z - qd) < N(d)$
- Since $z - qd \in I$, then $z = qd$ because $N(d)$ is minimal. Therefore $I \subset \langle d \rangle$