Some slides for 2nd Lecture, Algebra 2

Diego Ruano

Department of Mathematical Sciences
Aalborg University
Denmark

7-02-2013

A ring is an abelian group $(R, +)$ (the neutral element is 0) with an additional composition $\cdot$ called multiplication with satisfies (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 $(y + z) \cdot x = y \cdot x + z \cdot x$.

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

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 $x\lambda \in I$.

An ideal I in R that can be generated by one element is called a **principal ideal** (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**.

Proposition 3.1.10

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

Quotient Rings

- Let $I \subset R$ an ideal. In particular, $I \subset R$ is a subgroup for $+$
- We can consider left cosets $[x] = x + I$ and the set of left cosets
$$R/I = \{[x] : x \in R\}$$
- Recall: R/I is an abelian group (for "$+$"), $[x] = [y]$ if and only if $x - y \in I$ (see Lemma 2.2.6, page 63).

We can make R/I into a ring (for $[x], [y] \in R/I$):
$$[x] + [y] = [x + y]$$
$$[x][y] = [xy]$$
R/I is the quotient ring of R by I and has $[0]$ and $[1]$ as neutral elements for $+$ and $\cdot$.

We have that $[x] = [0]$ if $x \in$???

- One should proof that quotient ring of R by I is well defined: the proof is exactly the same as proposition 1.3.4.
- Example in $\mathbb{Z}$.

Proposition 3.2.2

Let $d \in \mathbb{N}$, $d \neq 0$, the group of units of $(\mathbb{Z}/d\mathbb{Z})^*$ is an abelian group with $\varphi(d)$ elements.

Proof: $[x] = x + d\mathbb{Z}$ is a unit if and only if $\gcd(x, d) = 1$.

- If $\gcd(x, d) = 1$ we use Euclidean algorithm: $\lambda x + \mu d = 1$.
- Then, $[\lambda x + \mu d] = [\lambda][x] = [1]$, hence x is a unit
- If $[x]$ is a unit in $\mathbb{Z}/d\mathbb{Z}$ then there exists $[\lambda] \in \mathbb{Z}/d\mathbb{Z}$ s.t. $[\lambda][x] = 1$.
- Then, $\lambda x - 1 \in d\mathbb{Z}$ and there is μ s.t. $\lambda x - 1 = \mu d$. And therefore $\gcd(x, d) = 1$ (exercise 1.14).

An element $x \in R$ is called a unit 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^*.

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

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

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

Proposition 3.2.3

Let $n \in \mathbb{N}$, then $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is a prime number. If n is a composite number then $\mathbb{Z}/n\mathbb{Z}$ is not a domain.
For a prime number p, the field $\mathbb{Z}/p\mathbb{Z}$ is denoted $\mathbb{F}_p$.

Proof:

- For $n = 0$, $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}$
- For $n > 0$, we have $|(\mathbb{Z}/n\mathbb{Z})^*| = \varphi(n)$ (by previous th.)
- However, $|\mathbb{Z}/n\mathbb{Z}| = n$. Therefore, $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if $\varphi(n) = n - 1$, that is, if n is prime.
- If $n = ab$ composite ($1 < a, b, < n$), we have $[a][b] = [0]$ but $[a], [b] \neq [0]$. Therefore it is not a domain.

Let $I \subset R$, with $I \neq R$, an ideal. If $xy \in I$ implies $x \in I$ or $y \in I$ (or both), for every $x, y \in R$, we say that I is a prime ideal.

Proposition 3.2.6

An ideal $I \subset R$ is a prime ideal if and only if R/I is a domain.

Proof:

- If I is prime, exercise 3.21 will show that R/I is a domain
- If R/I is a domain, then $R/I \neq 0$ and $[x][y] = 0$ implies $[x] = 0$ or $[y] = 0$, that is, $x \in I$ or $y \in I$.

Let $I \subset R$, with $I \neq R$, an ideal. If for $J \subset R$ ideal with $I \subsetneq J$ implies $J = R$, we say that I is a maximal ideal.

Proposition 3.2.7

An ideal $I \subset R$ is a maximal ideal if and only if R/I is a field. (Every maximal ideal is prime, because a field is a domain)

Proof (assume R/I is a field):

- Then $R/I \neq 0$ and for $[x] \neq 0$, there exists $[y]$ s.t. $[x][y] = [1]$.
- That is: for every $x \notin I$ there exists $y \in R$ such that $xy - 1 \in I$.
- Suppose J is another ideal s.t. $I \subset J \subset R$. If $x \in J \setminus I$, we may find $y \notin I$ s.t. $xy - 1 \in I \subset J$.
- But $x \in J$ and therefore $xy \in J$, hence $1 = -(xy - 1) + xy \in J$. So, $J = R$

Proof (assume $I \subset R$ is a maximal ideal):

- If $[x] \in R/I$ is non-zero, is it a unit?. We know that $x \notin I$.
- The subset $I + Rx = \{i + rx : i \in I, r \in R\}$ is an ideal in R.
- Since $I \subsetneq I + Rx$, we have that $I + Rx = R$ and therefore $1 \in I + Rx$
- So, $1 = m + rx$ for some $m \in I$ and $r \in R$.
- In R/I this means: $[1] = [r][x]$, and hence $[x]$ is a unit in R/I.

Example $\mathbb{Z}$

A map $f : R \to S$ between two rings R and S is called a ring homomorphism if:

1. It is a group homomorphism from $(R, +)$ to $(S, +)$.
2. $f(xy) = f(x)f(y)$, for every $x, y \in R$
3. $f(1) = 1$

A bijective ring homomorphism is called ring isomorphism. If $f : R \to S$ is an isomorphism, we say that R and S are isomorphic, $R \cong S$

Example: A surjective ring homomorphism

$$\begin{array}{ccc} R & \to & R/I \\ r & \mapsto & [r] \end{array}$$

Exercise 3.11

$\mathrm{Ker}(f) = \{r \in R : f(r) = 0\}$ is an ideal of R
The image $f(R)$ is a subring of S

Proposition 3.3.2

Let R, S be rings and $f : R \to S$ a ring homomorphism with kernel $K = \mathrm{Ker}(f)$. Then:

$$\begin{aligned} \tilde{f} : R/K &\to f(R) \\ r + K &\mapsto f(r) \end{aligned}$$

is a well defined map and a ring isomorphism

Proof:

- We know that $\tilde{f}$ is well defined and it is an isomorphism of abelian groups (theorem 2.5.1).
- $\tilde{f}((x+K)(y+K)) = \tilde{f}(xy+K) = f(xy) = f(x)f(y) = \tilde{f}(x+K)\tilde{f}(y+K)$
- $\tilde{f}(1+K) = f(1) = 1$