Some slides for 14th Lecture, Algebra

Diego Ruano

Department of Mathematical Sciences
Aalborg University
Denmark

4-11-2010

A 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 $(y + z) \cdot x = y \cdot x + z \cdot x$.

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 $x\lambda \in I$.

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:

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

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).
- $\tilde{f}((x+K)(y+K)) = \tilde{f}(xy+K) = f(xy) = f(x)f(y) = \tilde{f}(x+K)\tilde{f}(y+K)$
- $\tilde{f}(1+K) = f(1) = 1$

The unique ring homomorphism from $\mathbb{Z}$

Lemma 3.3.3

For every ring R, there is a unique ring hommorphism $f : \mathbb{Z} \to R$.

Proof: We use:

Proposition 2.6.1

Let G be group and $g \in G$. The map

$$\begin{aligned} f_g : \mathbb{Z} &\to G \\ n &\mapsto g^n \end{aligned}$$

is a group homomorphism from $(\mathbb{Z}, +)$ to G.

- Notation: $\langle g \rangle = f_g(\mathbb{Z}) = \{g^n : n \in \mathbb{Z}\}$
- $\mathrm{ord} = |\langle g \rangle|$ is called order of g

Characteristic

Let R be a ring.

- The characteristic of R is the order of 1 in R if $\mathrm{ord}(1)$ is finite.
- If the order of 1 is infinite, we say that R has characteristic zero.

In other words:

The characteristic of R is $n_1 \in \mathbb{N}$, where $n_1\mathbb{Z} = \mathrm{Ker}(f_1)$

Lemma 3.3.5

Let R be a ring. Then there is an injective ring homomorphism $\mathbb{Z}/n\mathbb{Z} \to R$, where $n = \mathrm{char}(R)$.

Proof:

Proposition 3.3.7

Let R be a domain. Then $\mathrm{char}(R)$ is either zero or a prime number.
If R is domain and is finite then R is a field and $\mathrm{char}(R)$ is a prime number

Proof:

- $\mathbb{Z}/n\mathbb{Z}$ is a subring of R and it should be also a domain. Then, n is zero or prime.
- If R is finite, $n > 0$.

Binomial formula

Lemma 3.3.8

Let R be a ring and a, b two elements in R. Then

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$$

Proof: Induction + trick:

$$\binom{n}{i} + \binom{n}{n-1} = \binom{n+1}{i}$$

We are also using $f(\mathbb{Z}) \subset R$

Theorem 3.3.9-Binomial formula with prime characteristic

Let R be a ring of prime characteristic p. Then

$$(x+y)^{p^r} = x^{p^r} + y^{p^r}$$

for every $x, y \in R$ and $r \in \mathbb{N}$.

Proof:

- $p | \binom{p}{i}$, for $i = 1, \ldots, p-1$
- $(x+y)^p = x^p + y^p$
- Induction on r:

$$(x+y)^{p^r} = ((x+y)^p)^{p^{r-1}} = (x^p + y^p)^{P^{r-1}} = (x^p)^{p^{r-1}} + (y^p)^{p^{r-1}}$$

Frobenius Map

Let R be a ring of prime characteristic, then F is a ring homomorphism:

$$\begin{array}{rcl} F : R & \to & R \\ x & \mapsto & x^p \end{array}$$

A relation R on a set S is a subset $R \subset S \times S$. We say xRy to mean $(x, y) \in R$.

A relation R on S is

- reflexive if xRx for every $x \in S$
- symmetric if $xRy \implies yRx$ for every $x, y \in S$
- transitive if xRy and $yRz \implies xRz$ for every $x, y, z \in S$

R is called equivalence relation if it is reflexive, symmetric and transitive.

Example: $I \subset R$ an ideal in a ring. We define the relation:

$$x \equiv y (\mathrm{mod}\ I) \iff x - y \in I$$

- Reflexive: $0 \in I$
- Symmetric: $x \in I \implies -x \in I$
- Transitive: $x, y \in I \implies x + y \in I$.

Let $\sim$ be an equivalence relation on a set S. Given $x \in S$, set

$$[x] = \{s \in S : s \sim x\} \subset S$$

This subset is called the equivalence class containing x and x is called a representative for $[x]$.
The set of equivalence classes $\{[x] : x \in S\}$ is denoted $S/\sim$.

Example: In the previous example $R/\sim$ is equal R/I, where $\sim$ is $\equiv$.

Compare page 225 and page 63

- Lemma A.2.3 and Lemma 2.2.6 (ii)
- Corollary A.2.4 and Lemma 2.2.6 (iii)
- Theorem A.2.6 and Corollary 2.2.7
- Definition A.2.7 and Example 2.2.4 (page 68)
- Theorem A.2.8 and Theorem 2.5.1 (page 71)