Some slides for 5th Lecture, Algebra 2

Diego Ruano

Department of Mathematical Sciences
Aalborg University
Denmark

16-02-2012

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: $x, y \in I \implies x + y \in I$.

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:

$$x \equiv y \pmod{I} \iff x - y \in I$$

- 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)

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)

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)

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)

Let $\sim$ be an equivalence relation on S and $x, y \in S$. Then $[x] = [y]$ if and only if $x \sim y$.

$[x] \cap [y] = \emptyset$ if $[x] \neq [y]$.

A partition of a set S is a collection $(S_i)_{i \in I}$ of subsets of S such that $\cup_{i \in I} S_i = S$, $S_i \cap S_j = \emptyset$ if $i \neq j$ and $S_i \neq \emptyset$.

Let S be a set with an equivalence relation $\sim$. Then the set of equivalence classes

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

is a partition of S. However, if $(S_i)_{i \in I}$ is a partition of S then we get an equivalence relation $\sim$ on S such that $S/\sim = (S_i)_{i \in I}$

Construction of the rational numbers

Proposition 3.4.1

Let R be a domain with field of fractions Q, let L be a field and let $\varphi : R \to L$ be an injective ring homomorphism. Then there exists a unique injective ring homomorphism $\overline{\varphi} : Q \to L$ such that $\overline{\varphi} \circ i = \varphi$.

Corollary 3.4.2

Let R be a domain contained in the field L. The smallest subfield in L containing R is

$$K = \{as^{-1} : a \in R, s \in R \setminus \{0\}\}$$

The field of fractions of R is isomorphic to K.

Proposition 3.4.1

Let R be a domain with field of fractions Q, let L be a field and let $\varphi : R \to L$ be an injective ring homomorphism. Then there exists a unique injective ring homomorphism $\overline{\varphi} : Q \to L$ such that $\overline{\varphi} \circ i = \varphi$.

Corollary 3.4.2

Let R be a domain contained in the field L. The smallest subfield in L containing R is

$$K = \{as^{-1} : a \in R, s \in R \setminus \{0\}\}$$

The field of fractions of R is isomorphic to K.

We assume from now on that R is a domain.

Suppose that $x, y \in R$. If $x = ry$ for some $r \in R$, we say that y is a divisor of x and we denote it by $y|x$

- $y|x$ if and only if $\langle x \rangle \subset \langle y \rangle$.
- If $x = uy$, where $u \in R^*$, then $\langle x \rangle = \langle y \rangle$.
- If $\langle x \rangle = \langle y \rangle$, then $x = ry$ and $y = sx$ for some s, r. Therefore $x = (rs)x$ and $rs = 1$. This implies that $r, s \in R^*$ and there exists $u \in R^*$ s.t. $x = uy$ and we say that x and y are associated elements of R.

Divisibility and greatest common divisor in a domain

We assume from now on that R is a domain.

Suppose that $x, y \in R$. If $x = ry$ for some $r \in R$, we say that y is a divisor of x and we denote it by $y|x$

- $y|x$ if and only if $\langle x \rangle \subset \langle y \rangle$.
- If $x = uy$, where $u \in R^*$, then $\langle x \rangle = \langle y \rangle$.
- If $\langle x \rangle = \langle y \rangle$, then $x = ry$ and $y = sx$ for some s, r. Therefore $x = (rs)x$ and $rs = 1$. This implies that $r, s \in R^*$ and there exists $u \in R^*$ s.t. $x = uy$ and we say that x and y are associated elements of R.

An element $d \in R$ is a greatest common divisor of $a, b \in R$ if d is a common divisor of a and b and every common divisor of a and b divides d.

Let R be a principal ideal domain. We know that for every $a, b \in R$ there is $d \in R$ s.t.

$$\langle a, b \rangle = \langle d \rangle$$

What is d?, d is the greatest common divisor of a and b.

Proof:

- d is a common divisor of a and b since $\langle a \rangle \subset \langle d \rangle$ and $\langle b \rangle \subset \langle d \rangle$
- If e is a common divisor of a and b, then $\langle e \rangle \supset \langle a, b \rangle = \langle d \rangle$. That is e divides d.

An element $d \in R$ is a greatest common divisor of $a, b \in R$ if d is a common divisor of a and b and every common divisor of a and b divides d.

Let R be a principal ideal domain. We know that for every $a, b \in R$ there is $d \in R$ s.t.

$$\langle a, b \rangle = \langle d \rangle$$

What is d?, d is the greatest common divisor of a and b.

Proof:

- d is a common divisor of a and b since $\langle a \rangle \subset \langle d \rangle$ and $\langle b \rangle \subset \langle d \rangle$
- If e is a common divisor of a and b, then $\langle e \rangle \supset \langle a, b \rangle = \langle d \rangle$. That is e divides d.