Algebra Definitions

eeleexx

June 25, 2024

Preface

The definitions included in this document are taken from the lecture notes by Dima Trushin. The original notes can be found in the GitHub repository at

`https://github.com/DimaTrushin/Algebra-DSBA`.

The repository is open to suggestions, and anybody is welcome to contribute by making pull requests at `https://github.com/eeleexx/AlgebraOralTest`. Don't hesitate to report any inconsistencies or errors in definitions, as well as if some of them are missing or blatantly incorrect.

A binary operation. Definition 4

Definition. *Suppose X is a set. A binary operation is a map $\circ : X \times X \to X$ by the rule $(x, y) \mapsto x \circ y$ for $x, y \in X$.*

In this case, the notation $\circ$ is the name of the operation. Simply speaking, the operation is a rule that takes two elements of the set X and produces a new element called $x \circ y$ of the same set X. This element $x \circ y$ is usually called the product of x and y.

Associative operation. Definition 7

Definition. *An operation $\circ : X \times X \to X$ is called associative if for every element $x, y, z \in X$ we have $(x \circ y) \circ z = x \circ (y \circ z)$.*

A neutral element. Definition 9

Definition. *Let $\circ : X \times X \to X$ be an operation on X. An element $e \in X$ is called neutral (or identity element) if for every element $x \in X$ we have $x \circ e = x$ and $e \circ x = x$.*

An inverse element in case of a binary operation. Definition 12

Definition. *Let $\circ : X \times X \to X$ be an operation such that there is a neutral element $e \in X$. An element $y \in X$ is called inverse to an element $x \in X$ if $x \circ y = e$ and $y \circ x = e$.*

A group. Definition 17

Definition. ***Definition of a group.***

- ***Data:***
  - *A set G.*
  - *An operation $\circ : G \times G \to G$.*
- ***Axioms:***
  - *The operation $\circ$ is associative.*
  - *The operation $\circ$ has a neutral element.*
  - *Every element $x \in G$ has an inverse.*

In this case, we say that the pair $(G, \circ)$ is a group. In order to simplify the notation, we usually say simply that G is a group assuming that the operation in use is clear. If in addition we have:

- *The operation $\circ$ is commutative.*

Then the group G is called abelian or simply commutative.

An abelian group. Definition 17

Definition. *Let G be a group with operation $\circ$. If the operation $\circ$ is commutative, that is, for every $x, y \in G$ we have $x \circ y = y \circ x$, then G is called an abelian group.*

The group $\mathbb{Z}_n$. Example 18 item 4

Definition. *Let n be any positive integer. The set $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ with addition modulo n is an abelian group. The operation on $\mathbb{Z}_n$ will be simply denoted by $+$.*

The group $\mathbb{Z}_n^*$. Example 18 item 5

Definition. *Let n be any positive integer. The set $\mathbb{Z}_n^* = \{m \in \mathbb{Z}_n \mid \gcd(m, n) = 1\}$ with multiplication modulo n is an abelian group. The operation on $\mathbb{Z}_n^*$ will be simply denoted by $\cdot$.*

A subgroup. Definition 19

Definition. *Let G be a group with operation $\circ$. A subset $H \subseteq G$ is called a subgroup if H itself forms a group with the inherited operation $\circ$ from G. This means that H must satisfy the group axioms: associativity, identity element, inverse elements, and closure under the operation $\circ$.*

A cyclic subgroup. Definition 22

Definition. *Let G be a group and $g \in G$ be an arbitrary element. The cyclic subgroup generated by g is the set $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$, where g^n denotes the n-th power of g (using the group operation $\circ$ repeatedly). In multiplicative notation, $g^n = g \circ g \circ \ldots \circ g$ (n times), and in additive notation, $ng = g + g + \ldots + g$ (n times).*

The order of an element of a group. Definition 24

Definition. *Let G be a group and $g \in G$ be an arbitrary element. Then there are two options:*

- *If $\operatorname{ord}(g) = \infty$, then the elements g^n and g^m are different whenever $n, m \in \mathbb{Z}$ are different.*
- *If $\operatorname{ord}(g) = n < \infty$, then elements $1, g, g^2, \ldots, g^{n-1}$ are different. In this case, the powers are repeated in cycles, that is in the series*

$$\ldots, g^{-2}, g^{-1}, 1, g, g^2, \ldots, g^{n-1}, g^n, g^{n+1}, \ldots, g^{2n-1}, g^{2n}, \ldots$$

are the same elements as $1, g, \ldots, g^{n-1}$ for any $k \in \mathbb{Z}$. In particular, $\langle g \rangle = \{1, g, \ldots g^{n-1}\}$.

A coset in a group. Definition 29

Definition. *Let G be a group, $H \subseteq G$ a subgroup, and $g \in G$ an arbitrary element. Then the set $gH = \{gh \mid h \in H\}$ is called the left coset of H with respect to g. In a similar way, we define right cosets. The set $Hg = \{hg \mid h \in H\}$ is called the right coset of H with respect to g.*

A normal subgroup. Definition 32

Definition. *Let G be a group and H its subgroup. The subgroup H is normal if its left and right cosets are the same, that is, $gH = Hg$ whenever $g \in G$.*

The index of a subgroup. Definition 38

Definition. *Let G be a finite group and $H \subseteq G$ a subgroup. Then the number of the left cosets of H is called the index of H and is denoted by $(G : H)$. This number also coincides with the number of right cosets of H.*

A homomorphism of groups. Definition 40

Definition. *Let G and H be groups. A homomorphism $\varphi : G \to H$ is a map such that $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$ for any $g_1, g_2 \in G$. In this case, φ is called a homomorphism from G to H.*

An isomorphism of groups. Definition 44

Definition. *Let G and H be groups. We define an isomorphism $\varphi : G \to H$.*

- ***Data:*** *A homomorphism $\varphi : G \to H$.*
- ***Axiom:*** *φ is bijective.*

In this case, φ is called an isomorphism between G and H. If there is an isomorphism between G and H, the groups G and H are called isomorphic.

The kernel of a homomorphism of groups. Definition 46 item 1

Definition. *Let $\varphi : G \to H$ be a homomorphism of groups. The kernel of φ is* $\ker \varphi = \{g \in G \mid \varphi(g) = 1\} \subseteq G$.

The image of a homomorphism of groups. Definition 46 item 2

Definition. *Let $\varphi : G \to H$ be a homomorphism of groups. The image of φ is* $\operatorname{Im} \varphi = \{\varphi(g) \mid g \in G\} = \varphi(G) \subseteq H$.

A product of groups. Definition 48

Definition. *Let G and H be groups. We define a new group $G \times H$ as follows:*

- *As a set, it is the product of the underlying sets of the groups: $G \times H = \{(g, h) \mid g \in G, h \in H\}$.*
- *The operation $\cdot : (G \times H) \times (G \times H) \to G \times H$ is given by the rule $(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$, for $g_1, g_2 \in G$ and $h_1, h_2 \in H$.*

The group $G \times H$ is called the product of the groups G and H.

A ring. Definition 60

Definition. *A ring is a set R equipped with two binary operations $+$ and $\cdot$ (addition and multiplication) such that:*

- *$(R, +)$ is an abelian group.*
- *$\cdot$ is associative.*
- *$\cdot$ is distributive over $+$.*

A field. Definition 60

Definition. *A ring is called a field if it satisfies the following conditions:*

- *Every non-zero element is invertible with respect to multiplication: for every $a \in R \setminus \{0\}$, there exists an element $b \in R$ such that $ab = ba = 1$.*
- $1 \neq 0$.

In this case, the inverse element for a is denoted by a^{-1}.

The ring $\mathbb{Z}_n$. Example 61 item 5

Definition. *The set of remainders modulo natural number n with the usual addition and multiplication modulo n, that is $(\mathbb{Z}_n, +, \cdot)$, is a commutative ring.*

A subring. Definition 63

Definition. *Let R be a ring. We are going to define a subring $T \subseteq R$.*

- ***Data:***
  - *A subset $T \subseteq R$.*
- ***Axioms:***
  - *$(T, +) \subseteq (R, +)$ is a subgroup.*
  - *T is closed under multiplication.*
  - *T contains 1.*

Invertible elements, zero divisors, nilpotent and idempotent elements. Definition 65

Definition. *Let R be a ring and $x \in R$ be an element of R.*

- *The element x is called invertible if there exists $y \in R$ such that $xy = yx = 1$. In this case y is denoted by x^{-1}. The set of all invertible elements of R is denoted by R^*.*
- *The element x is called left zero divisor if there exists a nonzero $y \in R$ such that $xy = 0$. Similarly, x is called right zero divisor if there exists a nonzero $y \in R$ such that $yx = 0$. The sets of left and right zero divisors will be denoted by $D_l(R)$ and $D_r(R)$, respectively. The set $D(R) = D_l(R) \cup D_r(R)$ is the set of all zero divisors of R.*
- *The element x is called nilpotent if $x^n = 0$ for some $n \in \mathbb{N}$. The set of all nilpotent elements is denoted by $\mathrm{nil}(R)$.*
- *The element x is called idempotent if $x^2 = x$. The set of all idempotents of R is denoted by $E(R)$.*

An ideal. Definition 67

Definition. *Suppose that $(R, +, \cdot)$ is a ring. An ideal I in the ring R is defined as follows:*

- ***Data:***
  - *A subset $I \subseteq R$.*
- ***Axioms:***
  - *$(I, +) \subseteq (R, +)$ is a subgroup.*

– *For any $r \in R$ we have*

$$rI = \{rx \mid x \in I\} \subseteq I \quad \text{and} \quad Ir = \{xr \mid x \in I\} \subseteq I$$

In this case, we say that I is an ideal of R. The subsets 0 and R are always ideals and are called the trivial ideals of R.

A homomorphism of rings. Definition 70

Definition. *Let $(R, +, \cdot)$ and $(S, +, \cdot)$ be rings. A homomorphism $\phi : R \to S$ is defined as follows:*

- ***Data:***
  - *A map $\phi : R \to S$.*
- ***Axioms:***
  - *$\phi(a + b) = \phi(a) + \phi(b)$ for all $a, b \in R$.*
  - *$\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in R$.*
  - *$\phi(1) = 1$.*

In this case, we say that ϕ is a homomorphism from R to S. If in addition ϕ is bijective, then ϕ is called an isomorphism, and R and S are called isomorphic.

The kernel of a ring homomorphism. Definition 74

Definition. *Let $\phi : R \to S$ be a homomorphism of rings. Then:*

- *The kernel of ϕ is $\ker \phi = \{r \in R \mid \phi(r) = 0\} \subseteq R$.*
- *The image of ϕ is $\operatorname{Im} \phi = \{\phi(r) \mid r \in R\} = \phi(R) \subseteq S$.*

A greatest common divisor of two polynomials. Definition 81

Definition. *Let F be a field and $f, g \in F[x]$ be some polynomials. A polynomial $d \in F[x]$ is called a greatest common divisor of f and g if:*

- *d divides both f and g.*
- *if h divides both f and g, then h divides d.*
- *d is monic.*

An irreducible polynomial in one variable. Definition 86

Definition. *A polynomial $f \in F[x] \setminus F$ is irreducible if for any $g, h \in F[x]$ such that $f = gh$, either g or h is a nonzero constant.*

The ring of polynomial remainders

Let F be a field and $f \in F[x]$ be any polynomial. I am going to define the ring $F[x]/(f)$. First, I need to specify a set, then two operations: addition and multiplication, and finally, I should check all the axioms. If $f = 0$, we define $F[x]/(f)$ to be the polynomial ring itself $F[x]$. The interesting case is when $f \neq 0$:

- $F[x]/(f) = \{g \in F[x] \mid \deg g < \deg f\}$ the set of remainders with respect to f.
- $+ : F[x]/(f) \times F[x]/(f) \to F[x]/(f)$ is the usual addition of polynomials.
- $\cdot : F[x]/(f) \times F[x]/(f) \to F[x]/(f)$ is the multiplication modulo f, namely: for every $g, h \in F[x]/(f)$, we define $gh \mod f$. The latter means, we divide gh by f with remainder and get $gh = qf + r$. Then the product of g and h is r.

The characteristic of a field. Definition 93

Definition. *Let F be a field. The characteristic of F is the minimal positive integer p such that*

$$\underbrace{1+1+\cdots+1}_{p \text{ times}} = 0.$$

If there is no such p, the characteristic is said to be zero. The characteristic of F is denoted by $\operatorname{char} F$.

To introduce a convenient notation, if we add an element $x \in F$ n times, where $n \in \mathbb{N}$, we may denote the sum as follows:

$$nx = \underbrace{x+x+\cdots+x}_{n \text{ times}}.$$

In particular, the characteristic of F is the smallest positive integer p such that $p \cdot 1 = 0$.

An extension by a root for fields. Section 7.2

nah i didnt find it

A lexicographical order on monomials. Definition 108

Definition. *We want to define a lexicographical order on monomials.*

1. *We need to fix an ordering on the variables $x_1, \ldots, x_n$. For example $x_1 > x_2 > \ldots > x_n$. However, we can take any permutation of the variables.*
2. *Suppose we fixed the ordering $x_1 > \ldots > x_n$ on the variables. Now, we are ready to define the corresponding lexicographical order Lex$(x_1, \ldots, x_n)$ on the monomials.*

Let $m = x_1^{k_1} \ldots x_n^{k_n}$ and $m' = x_1^{k_1'} \ldots x_n^{k_n'}$ be two monomials. Then we compare k_1 and k_1'. If $k_1 > k_1'$, then $m > m'$. If $k_1 < k_1'$, then $m < m'$. If $k_1 = k_1'$, then we compare k_2 and k_2' and repeat the algorithm above. In particular, $m > m'$ if and only if there exists $1 \leq j \leq n$ such that $k_1 = k_1', \ldots, k_{j-1} = k_{j-1}'$ and $k_j > k_j'$.

The leading term of a polynomial. Definition 113

Definition. *Suppose F is a field and we fix some lexicographical order on the monomials in n variables. As before, each polynomial $f \in F[x_1, \ldots, x_n]$ can be written as*

$$f = c_1 m_1 + c_2 m_2 + \ldots + c_k m_k,$$

$$c_i \in F, \; m_i \text{ are monomials such that } m_1 > m_2 > \ldots > m_k.$$

We denote its i-th largest monomial m_i by $M_i(f)$. In particular, $M_1(f)$ is the leading monomial of f, $M_2(f)$ is the next largest monomial of f etc. The i-th largest monomial need not exist if f contains less than i monomials.

An elementary reduction of a polynomial with respect to another one. Definition 114

Definition. *Suppose $g \in F[x_1, \ldots, x_n]$ is a nonzero polynomial and $f \in F[x_1, \ldots, x_n]$ is any polynomial. Assume that*

$$f = c_1 m_1 + \ldots + c_i m_i + \ldots + c_k m_k,$$

$$c_i \in F,\ m_i \text{ are monomials such that } m_1 > m_2 > \ldots > m_k$$

and

$$g = C(g)M(g) + g_0 = T(g) + g_0.$$

We take m to be m_i, that is a monomial in f, and assume that m is divisible by the leading monomial of g, that is $m = tM(g)$. We define an elementary reduction of f with respect to g as

$$f \xrightarrow{g} f' = f - \frac{c_i}{C(g)} tg.$$

The polynomial f' is the result of the elementary reduction.

In short, the elementary reduction works as follows: we find a monomial m_i of f divisible by $M(g)$ and replace it by the tail of g multiplied by $-\frac{c_i m_i}{T(g)}$.

A reduction and a remainder of a polynomial with respect to a set of nonzero polynomials. Definition 116

Definition. *Suppose $G \subseteq F[x_1, \ldots, x_n] \backslash \{0\}$ is a set of polynomials and $f, f' \in F[x_1, \ldots, x_n]$ are any polynomials. We say that f is reducible to f' with respect to G if there is a finite sequence of elementary reductions as below:*

$$f \xrightarrow{g_1} f_1 \xrightarrow{g_2} f_2 \xrightarrow{g_3} \ldots \xrightarrow{g_k} f_k = f' \quad \text{where } g_i \in G.$$

In this case, we will write

$$f \overset{G}{\rightsquigarrow} f'.$$

If the polynomial f' is not reducible by any $g \in G$, we say that f' is a remainder of f with respect to G.

Gröbner basis. Definition 118

Definition. *Suppose F is a field, $G \subseteq F[x_1, \ldots, x_n] \setminus \{0\}$, and we fix a lexicographical order on the monomials. We say that G is a Gröbner basis if for every $f \in F[x_1, \ldots, x_n]$ all its remainders are the same.*

S-polynomial. Definition 123

Definition. *Suppose F is a field, $f_1, f_2 \in F[x_1, \ldots, x_n]$ are some nonzero polynomials, and we are given a lexicographical order on monomials. Assume that*

$$f_1 = c_1 m_1 + f_1',$$

where $c_1 m_1$ is the leading term, and

$$f_2 = c_2 m_2 + f_2',$$

where $c_2 m_2$ is the leading term. Let m be the least common multiple of m_1 and m_2, then $m = m_1 t_1 = m_2 t_2$. Then, the polynomial

$$S_{f_1, f_2} = c_2 t_1 f_1 - c_1 t_2 f_2 = c_2 t_1 f_1' - c_1 t_2 f_2'$$

is called the S-polynomial of f_1 and f_2.

A finitely generated ideal. Definition 129

Definition. *Suppose F is a field and we are given a finite set of polynomials $g_1, \ldots, g_k \in F[x_1, \ldots, x_n]$. Then the set*

$$(g_1, \ldots, g_k) = \{g_1 h_1 + \ldots + g_k h_k \mid h_1, \ldots, h_k \in F[x_1, \ldots, x_n]\}$$

is an ideal of $F[x_1, \ldots, x_n]$ and is called the ideal generated by $g_1, \ldots, g_k$. If we take $G = \{g_1, \ldots, g_k\}$, then the ideal $(g_1, \ldots, g_k)$ is also denoted by (G) for short.