

algebra :: summary

I. integers.

I. i. well ordering principle. prime factorization.

def :: *natural numbers* ::

$$\mathbb{N} = \{0, 1, 2, \dots\}$$

def :: *a divides b* :: with $a, b \in \mathbb{Z}$ and $a \neq 0$,

$$\exists c \in \mathbb{Z} : b = ac \quad (\text{notation: } a|b)$$

def :: *prime* :: $p \in \mathbb{Z}^+$,

$$p > 1 \wedge \text{only } \{1, p\} | p$$

axiom :: *well-ordering* :: $\forall S \subseteq \mathbb{N} \setminus \{\emptyset\}$,

$$\exists s \in S : \forall n \in \mathbb{N}, s \leq n \quad (\text{least element})$$

axiom :: *induction* :: $S \subset \mathbb{N}$,

$$[0 \in S \wedge n \in S \Rightarrow n + 1 \in S]$$

$$\Rightarrow S = \mathbb{N}$$

th :: *fund. th. or arithmetic* :: any integer greater than 1 is a product of primes, and its prime factorization is unique

I. ii. euclidean division. bezout's identity.

def :: *gcd* :: $a, b, d, e \in \mathbb{Z}^*$,

$$d | \{a, b\} \wedge [e | \{a, b\} \Rightarrow e | d] \quad (\text{notation: } d = \gcd(a, b))$$

def :: *lcm* :: $a, b, l, m \in \mathbb{Z}^*$,

$$\{a, b\} | l \wedge [\{a, b\} | m \Rightarrow l | m] \quad (\text{notation: } l = \text{lcm}(a, b))$$

def :: *euler's totient* :: $a, n \in \mathbb{N}$,

$$P = \{a \in [1, n] : \gcd(a, n) = 1\} \subset \mathbb{N}$$

$$\Rightarrow \varphi(n) = |P| \quad (\text{notation : } \varphi(\cdot))$$

$$\text{:: remark :: } \gcd(n, m) = 1 \Rightarrow \varphi(nm) = \varphi(n)\varphi(m)$$

th :: *euclidean division* :: $n \in \mathbb{Z}, d \in \mathbb{Z}^+$,

$$\exists! q, r \in \mathbb{Z} : n = qd + r, \text{ with } r \in [0, d - 1]$$

lem :: $n, q \in \mathbb{Z}, d \in \mathbb{Z}^+$,

$$n = qd + r \Rightarrow \gcd(n, d) = \gcd(d, r)$$

corr :: $\forall a, b \in \mathbb{Z}^*$,

$$\exists x, y \in \mathbb{Z} : \gcd(a, b) = ax + by$$

corr :: $a, b \in \mathbb{Z}^*$ and $d = \gcd(a, b)$

$$ax + by = c, c \in \mathbb{Z}^* \text{ has integer solution} \Leftrightarrow c \in d\mathbb{Z}$$

:: remark :: *bezout's identity* :: with $d = 1$ we have: $\exists x, y \in \mathbb{Z} : ax + by = 1$

II. groups.

II. i. definitions.

def :: *group* :: set G with a binary operation $\cdot : G \times G \rightarrow G$ with:

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad (\text{associativity})$$

$$\exists e \in G : \forall a \in G, e \cdot a = a \cdot e = a \quad (\text{identity})$$

$$\forall a \in G, \exists a^{-1} \in G : a \cdot a^{-1} = a^{-1} \cdot a = e \quad (\text{inverse})$$

def :: *finite* ::

$$(G, \cdot) \text{ finite} \Leftrightarrow G \text{ finite}$$

def :: *abelian* :: $\forall a, b \in G,$

$$a \cdot b = b \cdot a \quad (\text{commutative})$$

def :: *order of group* ::

$$\text{order of } (G, \cdot) = |G| \quad (\text{notation: } |G|)$$

def :: *generators* :: (G, \cdot) and $S \subset G,$

$$\forall g \in G, \exists s_1 \dots s_k \in S : g = \prod s_i$$

def :: *relation in G* :: any equation $R : G \rightarrow G$ satisfied by all of G 's generators

def :: *presentation in S's and R's* :: set $S \subset G$ of generators of G and R_i the minimal set of relations,

$$\langle S \mid R_1 \dots R_k \rangle$$

def :: *order of element* :: $g \in G,$

$$\text{smallest } n \in \mathbb{N} : g^n = e \quad (\text{notation: } o(g))$$

:: remark :: $\nexists n \in \mathbb{N} : n = o(g) \Rightarrow o(g) = \infty \wedge G \text{ infinite}$

def :: *cyclic group* :: $|G| = k$

$$\exists g \in G : G = \{e, g, g^2, \dots, g^{k-1}\}$$

II. ii. group homomorphisms. subgroups. normal subgroups.

def :: *homomorphisms* :: $\phi : G \rightarrow H,$ with (G, \cdot_G) and $(H, \cdot_H),$

$$\forall x, y \in G, \phi(x \cdot_G y) = \phi(x) \cdot_H \phi(y)$$

:: remark :: *isomorphism* :: bijective homomorphism $\phi : G \rightarrow H$

:: remark :: *endomorphism* :: bijective homomorphism $\phi : G \rightarrow G$

def :: *kernel, image* :: $\phi : G \rightarrow H$

$$\ker(\phi) = \{g \in G : \phi(g) = e_H\}$$

$$\text{im}(\phi) = \{h \in H : \exists g \in G : \phi(g) = h\}$$

:: remark :: to check if $\phi : G \rightarrow H$ is a homomorphism, check that $\phi(s_G) \in H$ satisfy R_{G_i} , with $s_G \in S \subset G$ and R_{G_i} relations in G

def :: subgroup :: $H \subset G, H \neq \{\emptyset\} : (H, \cdot_G)$ is a group,

$$e_G \in H \quad (\text{identity})$$

$$\forall a, b \in H, a \cdot_G b \in H \quad (\text{stable wrt } \cdot_G)$$

:: remark :: $\phi : G \rightarrow H$ homomorphism $\Rightarrow \text{im}(\phi) \subset H$ (subgroup)

def :: normal subgroup :: $\forall g \in G, \forall h \in H,$

$$ghg^{-1} \in H \quad (\text{notation: } H \triangleleft G)$$

:: remark :: G abelian $\Rightarrow \forall H \subset G, H \triangleleft G$

:: remark :: $\phi : G \rightarrow H$ homomorphism $\Rightarrow \ker(\phi) \triangleleft G$

II. iii. dihedral group.

def :: dihedral group :: symmetries of a regular n -gon with composition operation \circ . $\forall n \geq 3$,

$$D_n = \langle r, s \mid r^n = e, s^2 = e, srs = r^{-1} \rangle$$

:: remark :: D_n is non-abelian

:: remark :: $|D_n| = 2n$

II. iv. cosets. lagrange's theorem.

def :: left coset wrt H in G :: subgroup $H \subset G$ and $g \in G$,

$$gH = \{gh, h \in H\} \subset G$$

:: remark :: H -cosets form a partition of G

:: remark :: H finite $\Rightarrow \forall x, y \in G \mid xH| = |yH|$

th :: lagrange's :: subgroup $H \subset G$ with G finite,

$$\exists k \in \mathbb{N} : |G| = k|H|$$

:: remark :: index of H in G :: $[G : H] := k = \frac{|G|}{|H|}$

corr :: G finite,

$$\forall g \in G, \exists k \in \mathbb{N} : |G| = ko(g)$$

corr :: G finite and $g \in G$,

$$g^{|G|} = e$$

corr :: G finite,

$$|G| = p \text{ prime} \Rightarrow G \text{ cyclic}$$

II. v. applications of lagrange's theorem.

def :: group of units in $\mathbb{Z}/n\mathbb{Z} :: (\mathbb{Z}/n\mathbb{Z}, \cdot)$,

$$((\mathbb{Z}/n\mathbb{Z})^*, \cdot) = \{x \in \mathbb{Z}/n\mathbb{Z} : \exists x^{-1} \in \mathbb{Z}/n\mathbb{Z}\} \quad (\text{invertible})$$

:: remark :: $[a]_n \in \mathbb{Z}/n\mathbb{Z}, [a]_n \neq [0]_n$,

$$[a]_n \text{ unit in } \mathbb{Z}/n\mathbb{Z} \Leftrightarrow \gcd(a, n) = 1$$

$$|(\mathbb{Z}/n\mathbb{Z})^*, \cdot| = \varphi(n)$$

:: remark :: $p \in \mathbb{Z}$ prime $\Rightarrow (\mathbb{Z}/p\mathbb{Z})^*, \cdot$ cyclic $\wedge |(\mathbb{Z}/p\mathbb{Z})^*, \cdot| = p - 1$

th :: fermat's little :: $p \in \mathbb{N}$ prime and $z \in \mathbb{Z}$,

$$p \nmid a \Rightarrow a^{p-1} \equiv 1 \pmod{p}$$

th :: euler's :: $a, n \in \mathbb{Z}^+$,

$$\gcd(a, n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$$

II. vi. quotient group.

def :: quotient group :: G and $N \triangleleft G$,

$$G/N = \{(xN), \forall x \in G\} \quad (\text{left } N\text{-cosets})$$

$$\text{with operation } (xN) \cdot_{G/N} (yN) = (xyN)$$

$$e_{G/N} = 1N \text{ and } (xN)^{-1} = x^{-1}N$$

:: remark :: $\phi : G \rightarrow H$ homomorphism, $G/\ker(\phi) \cong \text{im}(\phi)$

II. vii. symmetric group.

def :: G acts on $E :: (G, \cdot_G)$ finite group and E finite set,

$$\exists \cdot : G \times E \rightarrow E \quad \text{with}$$

$$\forall x \in E, e_G \cdot x = x \in E \quad (\text{identity})$$

$$\forall g_1, g_2 \in G, \forall x \in E, (g_1 \cdot g_2) \cdot x = g_1 \cdot (g_2 \cdot x) \quad (\text{associativity})$$

def :: orbit :: G acts on E with operation $\cdot, \forall x \in E$,

$$\text{orb}(x) = \{g \cdot x, g \in G\}$$

:: remark :: $|\text{orb}(x)| = 1 \Rightarrow x$ "fixed point"

:: remark :: $E = \cup_i \text{orb}(x_i) \wedge \text{orb}_i \cap \text{orb}_j = \emptyset$

def :: symmetric group :: $n \in \mathbb{N}, n \geq 1$

$$S_n = (\rho, \cdot_{S_n}) \quad \text{with}$$

$$\rho : \{1, \dots, n\} \rightarrow \{1, \dots, n\} \text{ injective } (\text{permutations})$$

$$e_{S_n} = \rho : \rho(i) = i \wedge \rho^{-1} : \rho^{-1}(\rho(i)) = i$$

:: remark :: the symmetric group of order n is the group of ρ 's of order n , and $|S_n| = n!$ is the order of the group itself

def :: k -cycle :: $\sigma \in S_n$ permutation and $\langle \sigma \rangle \subset S_n$ subgroup generated by σ ,

$$\begin{aligned} \exists ! i \in \{1 \dots n\} : |\text{orb}_\sigma(i)| \text{ non-trivial} &\in \{\sigma(i)\}_{i \in \{1 \dots n\}} \\ \Rightarrow \sigma \text{ } k\text{-cycle with } k &:= |\text{orb}_\sigma(i)| \end{aligned}$$

:: remark :: transposition :: 2-cycle

:: remark :: cycle notation :: $\pi \in S_n$ a k -cycle and $x \in \{1 \dots n\}$ in the non-trivial orbit of π , $\pi = (x \ \pi(x) \ \pi^2(x) \ \dots \ \pi^{k-1}(x))$ the cycle notation of π

def :: disjoint cycles :: $\pi_1, \pi_2 \in S_n$ k -cycles are disjoint if their non-trivial orbits don't intersect

:: remark :: disjoint cycles commute in S_n

def :: odd/even permutation :: $\pi \in S_n$ permutation and $\rho_i \in S_n$ transpositions ,

$$\pi = \rho_1 \cdot \rho_2 \cdot \dots \cdot \rho_r \begin{cases} \text{even if } r \text{ even} \\ \text{odd if } r \text{ odd} \end{cases}$$

th :: a permutation is a unique product of disjoint cycles, up to the order of factors

:: remark :: every k -cycle in S_n is a product of $k - 1$ transposition not necessarily disjoint

:: remark :: $(1 \ 2 \ \dots \ k) = (1 \ k)(1 \ k-1) \dots (1 \ 3)(1 \ 2)$

:: remark :: cycle decomposition :: $\pi, \rho \in S_n$, the cycle decomposition of $\pi\rho\pi^{-1}$ is obtained by replacing every i in the cycle decomposition of ρ by $\pi(i)$

corr :: S_n is generated by $\{(ij)\}_{1 \leq i < j \leq n}$

prop :: $A_n \subset S_n$,

$$A_n = \{\rho \text{ even}\} \Rightarrow A_n \triangleleft S_n \wedge [S_n : A_n] = 2$$

II. viii. orbit-stabilizer theorem.

def :: stabilizer :: G acting on E , $\forall x \in E$,

$$\text{stab}(x) = \{g \in G : g \cdot x = x\}$$

:: remark :: $\text{stab}(x)$, $x \in E$ is a subgroup of G

th :: orbit-stabilizer :: G acting on E and $\forall x \in E$,

$$|\text{orb}(x)| = [G : \text{stab}(x)]$$

II. ix. conjugacy classes. class equation.

def :: cycle type :: $\sigma \in S_n$ and $\sigma = \sigma_1 \dots \sigma_r$ disjoint cycle decomposition,

$$\{l \in \mathbb{N} : l_i = \text{length}(\sigma_i), 1 \leq i \leq r\}$$

def :: conjugacy class in G :: $\forall x, g \in G$,

$$\begin{aligned} g \cdot x &= gxg^{-1} \text{ (acts on itself by conjugation)} \\ \Rightarrow C_x &:= \text{orb}(x) \end{aligned}$$

:: remark :: $g_1, g_2 \in S_n$, cycle type₁ = cycle type₂ $\Leftrightarrow C_{g_1}^{S_n} = C_{g_2}^{S_n}$

:: remark :: $\forall x \in S_n, \exists$ bijection $C_x^{S_n} \rightarrow \text{cycle type}_x$

def :: centralizer :: $\forall x, g \in G,$

$$g \cdot x = gxg^{-1} \text{ (acts on itself by conjugation)} \\ \Rightarrow G_x := \text{stab}(x) \subset G$$

def :: center ::

$$Z(G) = \{x \in G : \forall g \in G, x \cdot g = g \cdot x\}$$

th :: class equation :: G finite and $\{x_i\}_{i=1}^m$ set of representatives of the $\{C_{x_i}\}_{i=1}^m$ containing more than one element,

$$|G| = |Z(G)| + \sum_{i=1}^m |C_{x_i}| \\ = |Z(G)| + \sum_{i=1}^m [G : G_{x_i}]$$

II. x. direct product of groups.

def :: direct product :: G, H groups, $G \times H$ a group with:

$$G \times H = \{(g, h) : g \in G, h \in H\} \text{ with} \\ \forall g_1, g_2 \in G, \forall h_1, h_2 \in H, (g_1, h_1) \cdot_{G \times H} (g_2, h_2) = (g_1 \cdot_G g_2, h_1 \cdot_H h_2) \\ e_{G \times H} = (e_G, e_H) \wedge (g, h)^{-1} = (g^{-1}, h^{-1})$$

:: remark :: $G \times H \cong H \times G$

:: remark :: $G \times H$ abelian $\Leftrightarrow G$ abelian $\wedge H$ abelian

:: remark :: $\{(e_G, h), h \in H\} \left\{ \begin{smallmatrix} \subset G \times H \text{ subgroup} \\ \cong H \end{smallmatrix} \right.$ and $\{(g, e_H), g \in G\} \left\{ \begin{smallmatrix} \subset G \times H \text{ subgroup} \\ \cong G \end{smallmatrix} \right.$

:: remark :: for cyclic groups, $C_n \times C_m \cong C_{nm} \Leftrightarrow \gcd(n, m) = 1$

:: remark :: $H, K \subset G$ subgroups, $\left. \begin{array}{l} H \cap K = \{e_G\} \\ \forall h \in H, \forall k \in K, hk = kh \\ \{hk, h \in H, k \in K\} \text{ span } G \end{array} \right\} \Rightarrow G \cong H \times K$

II. xi. classification of finite abelian groups.

def :: simple group ::

$$\nexists H \subset G \text{ subgroup} : H \neq \{e_G\} \text{ (non trivial)} \wedge H \neq G \text{ (not proper)}$$

th :: cauchy's :: G finite abelian,

$$p \in \mathbb{N} \text{ prime} : p | \text{order of } G \Rightarrow \exists g \in G : o(g) = p$$

corr :: G finite abelian,

$$\exists p \in \mathbb{N}, p \text{ prime} : G \cong C_p$$

def :: partition of n :: $n \in \mathbb{N},$

$$\{m_i \in \mathbb{N}, m_i \geq 1 : m_1 + \dots + m_k = n\}$$

prop :: G abelian, $n \in \mathbb{N}$ and p prime,

$$|G| = p^n \Rightarrow \exists! \{m_i \in \mathbb{N}\}_{1 \leq i \leq k \leq n} \text{ partition of } n : G \cong C_{p^{m_1}} \times \dots \times C_{p^{m_k}}$$

:: remark :: different partitions of n correspond to non-isomorphic abelian groups

prop :: G finite abelian and $p_1 \dots p_r$ distinct primes,

$$|G| = p_1^{n_1} \dots p_r^{n_r} \Rightarrow G \cong G_{p_1^{n_1}} \times \dots \times G_{p_r^{n_r}}$$

th :: *classification finite abelian groups* :: G finite abelian and $p_1 \dots p_r$ not necessarily distinct primes,

$$G \cong C_{p_1^{\alpha_1}} \times \dots \times C_{p_m^{\alpha_m}} \text{ with } |G| = p_1^{\alpha_1} \dots p_m^{\alpha_m}$$

:: remark :: *elementary divisors* :: the m -tuples $(p_1^{\alpha_1}, \dots, p_m^{\alpha_m})$ are elementary divisors of G

th :: G finite abelian and $|G| = d_1 \dots d_k$,

$$d_k | d_{k-1} \wedge \dots \wedge d_2 | d_1 \Rightarrow G \cong C_{d_1} \times \dots \times C_{d_k}$$

:: remark :: *invariant factors* :: the k -tuples (d_k, \dots, d_1) are the invariant factors of G