charlie mangano *18.02.2024*

algebra :: summary

I. integers.

I. i. well ordering principle. prime factorization.

def :: *natural numbers* ::

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

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

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

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

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

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

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

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

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

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

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

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

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

:: **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 $\cdot : G \times G \to G$ with:

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

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

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

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* ::

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

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

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

def :: *relation in* G :: any equation $R : G \to G$ 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,

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

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

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

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

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

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

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

def :: *homomorphisms* :: $\phi : G \to H$, 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 $\phi : G \to H$

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

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

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

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

:: **remark ::** to check if $\phi : G \to H$ 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 ::** $\phi : G \to H$ homomorphism $\Rightarrow \mathrm{im}(\phi) \subset H$ (subgroup)

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

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

:: **remark ::** G abelian $\Rightarrow \forall H \subset G, H \lhd G$

:: **remark ::** $\phi : G \to H$ homomorphism $\Rightarrow \ker(\phi) \lhd G$

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 $\Rightarrow \forall x, y \in G\ |xH| = |yH|$

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 $\Rightarrow (\mathbb{Z}/n\mathbb{Z})^*, \cdot)$ cyclic $\land$ $|(\mathbb{Z}/n\mathbb{Z})^*, \cdot)| = p - 1$

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* :: $a, n \in \mathbb{Z}^+$,

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

II. vi. quotient group.

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

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

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

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

:: **remark ::** $\phi : G \to H$ homomorphism, $G/\ker(\phi) \cong \operatorname{im}(\phi)$

II. vii. symmetric group.

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

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

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

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

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

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

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

:: **remark ::** $E = \cup_i \operatorname{orb}(x_i) \wedge \operatorname{orb}_i \cup \operatorname{orb}_j = \emptyset$

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

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

$$\rho : \{1, ...n\} \to \{1, ...n\} \text{ injective } \ \text{(permutations)}$$

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

:: **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,

$$\exists! i \in \{1 ... n\} : |\mathrm{orb}_\sigma(i)| \text{ non-trivial} \in \{\sigma(i)\}_{i \in \{1...n\}}$$
$$\Rightarrow \sigma \ k\text{-cycle with } k := |\mathrm{orb}_\sigma(i)|$$

:: **remark ::** *transposition* :: 2-cycle

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

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

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 ::** $(1 \ 2 \ ... \ k) = (1 \ k)(1 \ k - 1)...(1 \ 3)(1 \ 2)$

:: **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 :: $A_n \subset S_n$,

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

II. viii. orbit-stabilizer theorem.

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

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

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

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

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

II. ix. conjugacy classes. class equation.

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

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

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

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

:: **remark ::** $g_1, g_2 \in S_n$, cycle $\mathrm{type}_1 =$ cycle $\mathrm{type}_2 \Leftrightarrow C_{g_1}^{S_n} = C_{g_2}^{S_n}$

:: **remark ::** $\forall x \in S_n, \exists$ bijection $C_x^{S_n} \to$ cycle type_x

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

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

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 $\left\{C_{x_i}\right\}_{i=1}^m$ containing more than one element,

$$\begin{aligned}|G| &= |Z(G)| + \sum_{i=1}^{m} |C_{x_1}| \\ &= |Z(G)| + \sum_{i=1}^{m} \left[G : G_{x_i}\right]\end{aligned}$$

II. x. direct product of groups.

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

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

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

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

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

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

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

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* :: $n \in \mathbb{N}$,

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

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

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

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

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

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

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

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

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

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

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

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