charlie mangano *24.01.2025*

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

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

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

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

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

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

cor :: $a, b \in \mathbb{Z}^*$ 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 multiplicative binary operation $\cdot : G \times G \to G$ with:

$$\forall a, b, c \in G, (a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \text{(associativity)}$$

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

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

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 $S \subset G$,

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

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* :: $g \in G$,

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

:: **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* :: $[G : H] := k = \frac{|G|}{|H|}$

cor :: G finite,

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

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

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

cor :: 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 $\wedge$ $|(\mathbb{Z}/n\mathbb{Z})^*, \cdot)| = p - 1$

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 $N \lhd G$,

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

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

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

:: **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,

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

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

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

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

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

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

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

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

:: **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,

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

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

:: **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 $\pi(i)$

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

prop :: $A_n \subset S_n$,

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

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

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

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

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

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

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

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 $\left\{C_{x_i}\right\}_{i=1}^m$ 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:

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

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

:: **remark** :: $G \times H$ abelian $\Leftrightarrow G$ abelian $\land$ 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, $\left.\begin{array}{r} H\cap K = \{e_G\} \\ \forall h\in H, \forall k \in K, hk = kh \\ \{hk, h\in H, k\in K\} \text{ span } G\end{array}\right\} \Rightarrow G \cong H \times K$

II. xi. classification of finite abelian groups.

def :: *simple group* ::

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

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

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

cor :: 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 $|G| = d_1 ... d_k$,

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

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

III. rings.

III. i. definitions.

def :: *ring* :: set A with multiplicative and additive binary operations $(A, \cdot, +)$ with

$$A \text{ abelian wrt } + \begin{cases} \forall a, b, c \in A, (a + b) + c = a + (b + c) & \text{(associativity)} \\ \exists e_+ \in A : \forall a \in A, e_+ + a = a + e_+ = a & \text{(identity)} \\ \forall a \in A, \exists (-a) \in A : a + (-a) = (-a) + a = e_+ & \text{(inverse)} \\ \forall a, b \in A, a + b = b + a & \text{(commutative)} \end{cases}$$

$$A \text{ group wrt } \cdot \begin{cases} \forall a, b, c \in A, (a \cdot b) \cdot c = a \cdot (b \cdot c) & \text{(associativity)} \\ \exists e_. \in A : \forall a \in A, e_. \cdot a = a \cdot e_. = a & \text{(identity)} \\ \forall a \in A, \exists a^{-1} \in A : a \cdot a^{-1} = a^{-1} \cdot a = e_. & \text{(inverse)} \end{cases}$$

$$\forall a, b, c \in A, (a + b) \cdot c = a \cdot c + b \cdot c \quad \text{(distributivity)}$$

def :: *commutative* :: $\forall a, b \in A$,

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

def :: *subring* :: additive subgroup, closed wrt multiplication and containing $e_.$

III. ii. zero divisors. integral domains.

def :: *left/right zero divisor* :: A ring, $a \in A$,

$$\exists x \in A, x \neq e_+ : ax = e_+ \quad \text{(left zero divisor)}$$

$$\exists x \in A, x \neq e_+ : xa = e_+ \quad \text{(right zero divisor)}$$

:: **remark** :: *two-sided zero divisor* :: $x \in A$ both right and left zero divisor

:: **remark** :: $\forall A$ ring, e_+ two-sided zero divisor

:: **remark** :: $x \in A$ zero divisor, A commutative $\Rightarrow x$ two-sided

def :: *domain* :: A ring,

$$\nexists x \in A : x \text{ trivial zero divisor} \Rightarrow A \text{ domain}$$

def :: *integral domain* :: A ring,

$$A \text{ domain} \wedge A \text{ commutative}$$

:: **remark** :: $A = \mathbb{Z}/n\mathbb{Z}$, A integral domain $\Leftrightarrow n$ prime

:: **remark** :: A domain $\Leftrightarrow \forall a, b, c \in A, \begin{cases} ab = ac \wedge a \neq 0 \Rightarrow b = c \\ ba = ca \wedge a \neq 0 \Rightarrow b = c \end{cases}$

def :: *division ring* :: ring A,

$$\forall a \in A, a \neq 0, \exists b \in A : a \cdot b = b \cdot a = e_. \quad \text{(inverse)}$$

:: **remark** :: equivalent to: A ring where $A \setminus \{e_+\}$ group wrt $\cdot$

:: **remark** :: A division ring $\Rightarrow$ A domain

def :: *field* :: commutative division ring

cor :: $A = \mathbb{Z}/n\mathbb{Z}, A$ field $\Leftrightarrow n$ prime

III. iii. ideals.

def :: *left/right ideal* :: $I \subset A$,

$$I \text{ subgroup wrt } + \wedge \begin{cases} \forall x \in I, \forall a \in A, a \cdot x \in I & \text{(left ideal)} \\ \forall x \in I, \forall a \in A, x \cdot a \in I & \text{(right ideal)} \end{cases}$$

:: **remark** :: *two-sided ideal* :: $I \subset A$ both left and right ideal

:: **remark** :: $I \subset A$ ideal, A commutative $\Rightarrow I$ two-sided

:: **remark** :: $\forall A$ ring, $\{e_+\} \subset A$ and $A \subset A$ ideals

:: **remark** :: $\forall I \subset A$ ideal, $e_+ \in I$

prop :: *ideal properties* :: A commutative ring and $I, J \subset A$ ideals,

$$e_\cdot \in I \Rightarrow I = A$$
$$I \cap J \subset A \text{ ideal}$$
$$I \cup J \subset A \text{ not necessarily ideal}$$
$$\{x + y\}_{x \in I, y \in J} \subset A \text{ ideal} \quad (\text{notation: } I + J)$$
$$\{a \cdot x \cdot y, x \in I, y \in J, a \in A\} \subset A \text{ ideal} \quad (\text{notation: } I \cdot J)$$

def :: *ideal generated by S* :: $S \subset A$ set,

$$(S) = \bigcap_{I_i \subset A \text{ ideals}} I_i \subset A$$
$$A \text{ commutative} \Rightarrow (S) = \{a \cdot s, \forall a \in A, \forall s \in S\} \subset A$$

th :: A commutative,

$$\nexists I \subset A \text{ ideal} : I \neq \{e_+\} \wedge I \neq A \Leftrightarrow A \text{ field}$$

def :: *principal* :: A commutative and $I \subset A$ ideal,

$$I = (x), x \in A$$

def :: *prime* :: A commutative and $I \subset A$ ideal,

$$\forall a, b \in A, a \cdot b \in I \Rightarrow a \in I \vee b \in I$$

def :: *maximal* :: A commutative and $I \subset A$ proper ideal,

$$\nexists J \subset A \text{ proper ideal} : I \subset J \text{ proper subset}$$

III. iv. equivalence and congruence relations. quotient ring.

def :: *equivalence relation* :: E set and $x \sim y$ relation on E,

$$\forall x \in E, x \sim x \quad \text{(reflexive)}$$
$$\forall x, y \in E, x \sim y \Rightarrow y \sim x \quad \text{(symmetric)}$$
$$\forall x, y, z \in E, x \sim y \wedge y \sim z \Rightarrow x \sim z \quad \text{(transitive)}$$

def :: *equivalence class* :: E set and $x \in E$,

$$\bar{x}_E = \{y \in E : x \sim y\} \subset E$$

:: **remark** :: *quotient set* :: E set, $E/\sim \; = \{\bar{x}_E, \forall x \in E\}$

:: **remark** :: E set, $\forall x, y \in E, x \neq y \Rightarrow \bar{x} = \bar{y} \vee \bar{x} \cap \bar{y} = \emptyset$

def :: *congruence relation* :: A commutative and $\sim$ equivalence relation,

$$\forall a, b, c, d \in A, a \sim b \wedge c \sim d \Rightarrow a + c \sim b + d \wedge a \cdot c \sim b \cdot c$$

prop :: A commutative and $\sim$ congruence relation,

$$e_+ \nsim e_. \Rightarrow A/\sim \text{ structure of commutative ring}$$

:: **remark** :: A commutative ring and $I \subset A$ ideal, $a \sim b \Leftrightarrow (a - b) \in I$ congruence relation in A

:: **remark** :: A commutative ring and $\sim$ congruence relation, $I = \{a \in A, a \sim e_+\}$ ideal

def :: *quotient ring* :: A commutative ring, $I \subset A$ ideal,

$$A/I \text{ set of congruence classes modulo ideal } I$$

III. v. ring $\mathbb{Z}$.

def :: *principal ideal ring/domain* :: A commutative ring/integral domain where every ideal is principal

:: **remark** :: ring $\mathbb{Z}$ is a principal ideal domain

cor :: $I = (\{a_1, ..., a_n\}) \subset \mathbb{Z}$ ideal,

$$I = (d) \subset \mathbb{Z} \text{ where } d = \gcd(a_1, ..., a_n)$$

III. vi. homomorphisms. characteristics of rings. direct products of rings.

def :: *ring homomorphism* **::** A, B rings and $f : A \to B$ mapping, $\forall x, y \in A$,

$$f(x +_A y) = f(x) +_B f(y)$$
$$f(x \cdot_A y) = f(x) \cdot_B f(y)$$
$$f(e_{+,A}) = e_{+,B} \wedge f(e_{\cdot,A}) = e_{\cdot,B}$$

prop :: A, B commutative rings and $f : A \to B$ homomorphism,

$$\ker(f) = \{a \in A : f(a) = e_+\} \subset A \text{ ideal}$$
$$\text{im}(f) \subset B \text{ subring}$$

prop :: $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ ring homomorphism,

$$m \mid n \wedge f([a]_n) = [a]_m$$

prop :: A ring,

$$\exists! \tau : \mathbb{Z} \to A \text{ ring homomorphism, and}$$
$$\ker(\tau) = \{e_+\} \vee \ker(\tau) = d \in \mathbb{Z}^+$$

def :: *characteristic* **::** A ring and $\tau : \mathbb{Z} \to A$ unique ring homomorphism,

$$c_A = \begin{cases} e_+ & \text{if} \ker(\tau) = \{e_+\} \\ d & \text{if} \ker(\tau) = (d) \end{cases}$$

:: **remark ::** $c_A = mk \in \mathbb{Z}^+ : m, k \geq 2 \Rightarrow \exists$ non-trivial zero divisors $\in A$

cor :: A field $\Rightarrow c_A = e_+ \vee c_A = p, p$ prime

:: **remark ::** $\exists A$ not a field : $c_A = p, p$ prime

def :: *direct product* **::** A, B rings,

$$A \times B = \{(a, b), a \in A, b \in B\}$$
$$e_{+,A\times B} = (e_{+,A}, e_{+,B}) \wedge e_{\cdot,A\times B} = (e_{\cdot,A}, e_{\cdot,B})$$

prop :: A, B commutative rings,

$$c_A \neq e_+ \wedge c_B \neq e_+ \Rightarrow c_{A\times B} = \text{lcm}(c_A, c_B)$$

III. vii. chinese remainder theorem.

th :: A commutative ring and $I, J \subset A$ ideals,

$$I + J = A \Rightarrow \exists f : A/(I \cap J) \to A/I \times A/J \text{ ring isomorphism}$$
$$\text{and } f : \bar{x}_{I \cap J} \to (\bar{x}_I, \bar{x}_J)$$

cor :: $m, n \in \mathbb{Z}$ and $\gcd(m, n) = 1$,

$$\forall a_1, a_2 \in \mathbb{Z}, \exists a \in \mathbb{Z} : a \equiv a_1 (\operatorname{mod} m) \wedge a \equiv a_2 (\operatorname{mod} n)$$
$$a \text{ solution} \Rightarrow \{a + mn\mathbb{Z}\} \text{ solutions}$$

th :: $d_1, ..., d_n \in \mathbb{Z} : \forall i \neq j, \gcd\left(d_i, d_j\right) = 1$ and $d = d_1 ... d_n$,

$$f : \mathbb{Z}/(d) \to \mathbb{Z}/(d_1) \times ... \times \mathbb{Z}/(d_n)$$
$$f([a]_d) = \left([a]_{d_1}, ..., [a]_{d_n}\right)$$

cor :: $d_1, ..., d_n \in \mathbb{Z} : \forall i \neq j, \gcd\left(d_i, d_j\right) = 1$ and $d = d_1 ... d_n$,

$$\forall a_1, ..., a_r \in \mathbb{Z}, \exists a \in \mathbb{Z} : \begin{cases} a \equiv a_1 (\operatorname{mod} d_1) \\ ... \\ a \equiv a_r (\operatorname{mod} d_r) \end{cases}$$
$$a \text{ solution} \Rightarrow \{a + d\mathbb{Z}\} \text{ solutions}$$

III. viii. polynomials in one variable with coefficients in commutative ring

def :: *ring of polynomials* **::** A commutative ring,

$$A[x] = \{a_0 + a_1 x + ... + a_n x^n, n \in \mathbb{N}, a_i \in A\}$$
$$= \{(a_0, a_1, ...)\}_{a_i \in A} : a_i = 0 \text{ for large } i \in \mathbb{N}$$

:: **remark ::** $A[x]$ commutative ring

def :: *degree* **::** $f(x) \in A[x]$ non-trivial,

$$\deg(f(x)) = n \text{ largest} : a_n \neq 0$$

:: **remark ::** a_n dominant coefficient and a_0 constant term

:: **remark ::** $f(x) = 0 \Rightarrow \deg(f) := -\infty$

prop :: $A[x]$ ring and $f, g \in A[x]$

$$\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$$
$$A \text{ integral domain} \Rightarrow \deg(f \cdot g) = \deg(f + g)$$

th :: A integral domain,

$$A[x] \text{ integral domain}$$
$$\text{invertible elements} \in A[x] = \text{invertible elements} \in A$$

th :: F field, $f, d \in F[x]$ and $\deg(d) \geq 1$,

$$\exists q, r \in F[x] : f(x) = q(x)d(x) + r(x) \text{ with}$$
$$r(x) = 0 \vee \deg(r) < \deg(d)$$

III. ix. euclidean domains. principal ideal domains.

def :: *euclidean domain* **::** A integral domain,

$$\exists \nu : A \setminus \{e_+\} \to \mathbb{N} : \forall a, b \in A, b \neq e_+, \exists q, r \in A : a = qb + r$$
$$r = e_+ \vee \nu(r) < \nu(b)$$

:: **remark ::** F field $\Rightarrow F[x]$ euclidean domain

th ::

$$A \text{ euclidean domain} \Rightarrow A \text{ principal ideal domain}$$

cor ::

$$F \text{ field} \Rightarrow F[x] \text{ principal ideal domain}$$

def :: *associates* **::** A integral domain and $a, b \in A$,

$$b = au, u \in A^*$$
$$a = bv, v \in A^*$$

:: **remark ::** ideals generated by associates are the same

prop :: A integral domain, $\forall a, b, d_1, d_2, l_1, l_2 \in A$,

$$d_1, d_2 = \gcd(a, b) \Rightarrow d_1, d_2 \text{ associates}$$
$$l_1, l_2 = \operatorname{lcm}(a, b) \Rightarrow l_1, l_2 \text{ associates}$$

:: **remark ::** *bezout's theorem* :: E euclidean domain, $d = \gcd(a, b) \Rightarrow (a) + (b) = (d)$ ideal $\subset E$

:: **remark ::** $a, b, c \in E$ euclidean domain, $\gcd(a, b) = 1 \wedge a|bc \Rightarrow a|c$ and $\gcd(a, b) = 1 \wedge \gcd(a, c) = 1 \Rightarrow \gcd(a, bc) \Rightarrow 1$

:: **remark ::** $a, b, c \in E$ euclidean domain, $\gcd(a, b) = 1 \wedge a|c \wedge b|c \Rightarrow ab|c$ and $\gcd(a, b) = 1 \Rightarrow \operatorname{lcm}(a, b) = ab$

:: **remark ::** $(a) \cap (b) = (m)$ ideal $\subset E$, with $m = \operatorname{lcm}(a, b)$

III. x. chinese remainder theorem for euclidean domain.

th :: A euclidean domain and $m = m_1 ... m_r$ with $\gcd(m_i, m_j) = 1$,

$$f : A/(m) \to A/(m_1) \times ... \times A/(m_r) \text{ isomorphism, with}$$
$$f\left(\bar{x}_{(m)}\right) = \left(\bar{x}_{(m_1)}, ..., \bar{x}_{(m_r)}\right)$$

cor :: *chinese remainder theorem for polynomial rings* :: F field and $f_1(x), ..., f_{r(x)}$ polynomials in $F[x]$,

$$\gcd(f_i, f_j) = 1$$
$$\Rightarrow \exists \Phi : F[x]/(f_1 \cdot ... \cdot f_r) \to F[x]/(f_1) \times ... \times F[x]/(f_r) \text{ isomorphism}$$

III. xi. irreducible elements in euclidean domains.

def :: *irreducible* :: A integral domain and $a, b, c \in A$,

$$c \notin A^* \wedge c \neq e_+ \wedge [c = ab \Rightarrow a \in A^* \vee b \in A^*]$$

th :: A principal ideal domain,

$$p \in A \text{ irreducible} \Leftrightarrow p \neq e_+ \wedge (p) \subset A \text{ maximal}$$

prop :: $a, b \in A$ euclidean domain and $I = (a) \subsetneq A$ non-trivial,

$$\bar{b} \in (A/I)^* \Leftrightarrow \gcd(a, b) = 1$$
$$\bar{b} \in A/I \text{ non-trivial zero divisor} \Leftrightarrow b \notin I \wedge \gcd(a, b) \neq 1$$
$$A/I \text{ field} \Leftrightarrow a \in A \text{ irreducible}$$

cor :: F field and $f \in F[x]$ non-trivial polynomial,

$$F[x]/(f) \text{ field} \Leftrightarrow f \text{ irreducible in } F[x]$$

:: **remark** ::

$$\begin{array}{ccccccccc} & & & & \text{division ring} & \subset & \text{domain} & \subset & \text{ring} \\ \text{field} & \subset & \text{euclidean domain} & \subset & \text{principal ideal domain} & \subset & \text{integral domain} & \subset & \text{commutative ring} \end{array}$$

:: **remark** :: $\mathbb{Z}[x] \wedge F[x, y]$ with F field are integral domains

:: **remark** :: n not prime, $\mathbb{Z}/n\mathbb{Z}$ and $(\mathbb{Z}/n\mathbb{Z})[x]$ not integral domains

III. xii. quotient of polynomial rings.

prop :: F field and $f \in F[x]$ polynomial,

$$\deg(f) = 1 \Rightarrow f \text{ irreducible}$$
$$\deg(f) = 2 \vee \deg(f) = 3, f \text{ irreducible} \Leftrightarrow \text{no root} \in F$$

prop :: $\alpha = \frac{r}{s} \in \mathbb{Q}$ root of $f \in \mathbb{Z}[x]$,

$$s | a_n \wedge r | a_0$$

prop :: *eisenstein's criterion* **::** $f \in \mathbb{Z}[x]$ polynomial with $\gcd(a_0, ..., a_n) = 1$,

$$p \in \mathbb{Z} : p \mid \{a_0, ..., a_{n-1}\} \wedge p \nmid a_n \wedge p^2 \nmid a_0 \Rightarrow f \text{ irreducible in } \mathbb{Q}[x] \text{ and } \mathbb{Z}[x]$$

prop :: F field and $f \in F[x]$ irreducible polynomial with $\deg(f) = n \geq 1$,

$$K = F[x]/(f) \text{ field} : \forall a \in K, a = a_0\overline{1} + ... + a_{n-1}\overline{x^{n-1}}$$
$$\text{where } a_i \in F \wedge \overline{x^i} \text{ congruence class } x^i + (f)$$

cor :: F field, $|F| = q$ and $f \in F[x]$ irreducible polynomial,

$$\deg(f) \coloneqq n \geq 1 \Rightarrow |F[x]/(f)| = q^n$$

III. xiii. finite fields.

def :: *notation* **::** $p \in \mathbb{N}$ prime,

$$\mathbb{F}_p \equiv \mathbb{Z}/p\mathbb{Z}$$

prop :: K field and $n \in \mathbb{N}^+$,

$$|K| = p^n \Rightarrow c_K = p$$

prop :: A field,

$$|A| = p \Rightarrow A \cong \mathbb{F}_p$$

prop :: K field,

$$c_K = p \Rightarrow \exists L \text{ subfield} \subset K : L \cong \mathbb{F}_p$$

prop :: K finite field,

$$c_K = p \Rightarrow \exists n \in \mathbb{N}^+ : |K| = p^n$$

prop :: F field and $f \in F[x]$ polynomial,

$$\exists K \text{ field} : F \subset K \wedge \text{roots of } f \in K$$

prop :: K finite field,

$$K^* \text{ cyclic}$$

th :: p prime and $n \in \mathbb{N}, n > 1$,

$$\exists! K \text{ field} : |K| = p^n$$
$$\exists f \in \mathbb{F}_p[x] \text{ irreducible} : \mathbb{F}_p[x]/(f) \cong K$$

cor :: $\forall n \in \mathbb{N}^+, \forall p$ prime,

$$\exists f \in \mathbb{F}_p[x] \text{ irreducible} : \deg(f) = n$$

prop :: $\forall n \in \mathbb{N}^+, \forall p$ prime,

$$\exists! \mathbb{F}_{p^n} \text{ finite field} : |\mathbb{F}_{p^n}| = p^n \wedge c_{\mathbb{F}_{p^n}} = p$$