—3—

–Napiš Čínskou větu o zbytcích (pro $\mathbb{Z}_n$).

$n_1, ..., n_k \in \mathbb{N}$ po dvou nesoudělná, $n = n_1 \cdot \ldots \cdot n_k$. Pak zobr. f: $\mathbb{Z}_n \to \prod_{i=1}^{k} \mathbb{Z}_{n_i}$ dané předpisem $f(x) = (x \mod n_1, \ldots, x \mod n_k)$ je bijekce slučitelná s operacemi + a ·.

–Definuj Eulerovu fci a uveď vzorec pro její výpočet.

zobr. $\varphi : \mathbb{N} \to \mathbb{N}$, tž. $\varphi(n) = |0 < k < n | NSD(k, n) = 1|$

$\varphi(\prod_{i=1}^{k} p_i^{r_i}) = \prod_{i=1}^{k} \varphi(p_i^{r_i}) = \prod_{i=1}^{k} (p_i - 1) p_i^{r_i - 1}$ Eulerovu

–Definuj Eulerovu fci a napiš Malou Fermatovu větu.

zobr. $\varphi : \mathbb{N} \to \mathbb{N}$, tž $\varphi(n) = |0 < k < n | NSD(k, n) = 1|$

$1 < a, n \in \mathbb{N}$ nesoudělná: $(a^{\varphi(n)}) \mod n = 1$.

–Pro daný monoid $M(\cdot)$, definuj grupu $M^*(\cdot)$ invertibilních prvků.

$M^* = a \in M | \exists b \in M : a \cdot b = b \cdot a = 1$

–Uveď nějaký postup na výpočet inverzního prvku v grupě invertibilních prvků $\mathbb{Z}_n^*(\cdot)$.

Eukleidův alg: $x \cdot a + y \cdot n = 1$, $a^{-1} = x$

–Definuj grupu invertibilních prvků $\mathbb{Z}_n^*(\cdot)$ monoidu $\mathbb{Z}(\cdot)$. Které obsahuje prvky? Zn

$\mathbb{Z}_n^* = x \in \mathbb{Z}_n | NSD(x, y) = 1$??????????????????

–Napiš nějakou množinu generátorů grupy permutací $\mathbf{S}_n(\circ)$ velikosti $\leq n^2$.

všechny transpozice (každá permutace se dá na ně rozložit) nebo {(1 2 3 ... n), (1 2)} - lze jejich skládáním získat libovolná transpozice

–Napiš nějakou množinu generátorů grupy sudých permutací $\mathbf{A}_n(\circ)$ velikosti $\leq n^3$.

trojcykly ??????????????

–Uveď df grupy a nějaký příklad grupy, která není komutativní.

množina s asoc. bin. operací, v množině leží neutrální prvek a každý prvek této množiny je invertibilní

čtvercové regulární matice nad tělesem T; $\mathbf{S}_n(\circ)$ T^(n x n)(*) pro n > 2

–Uveď df komutativní grupy a řekni, které podgrupy komutativní grupy jsou normální.

množina s asoc. komut. bin. operací, v množině leží neutr. prvek a každý prvek je invertibilní

všechny

–Uveď df grupy a podgrupy.

grupa = množina s asoc. bin. operací, v množině leží neutrální prvek a každý prvek této množiny je invertibilní

podgrupa = množina H tž: $\emptyset \neq H \subseteq G$, uzavřená na ·, $\forall h \in H : h^{-1} \in H$

–Uveď df monoidu a př monoidu, který není grupou.

množina s asoc. bin. operací, v množině leží neutr. prvek

matice $n \times n$ nad tělesem T s operací násobení (neutr.: I_n, ale není inverzní prvek) nebo "slovní monoid": {epsilon, a, b, c, ...}(operace zřetězení)

neutrální: epsilon

—4—

–Napiš, co rozumíme faktorovou grupou grupy $G(\cdot)$ podle normální podgrupy H.

$G/H(\cdot)$, kde $H = [1]_\rho$, $[a]_\rho \cdot [b]_\rho = [a \cdot b]_\rho$

–Napiš, co rozumíme ekvivalencí $rmodH$ na grupě $G(\cdot)$, kde H je její podgrupa.
$(a,b) \in rmodH \Leftrightarrow a \cdot b^{-1} \in H$
–Napiš Lagrangeovu větu. Co přesně značí $[G:H]$?
H podgrupa grupy $G(\cdot)$, pak $|G| = [G:H] \cdot |H|$.
index podgrupy H v grupě G: $[G:H] = |G/rmodH|$
–Jaký je vztah řádu grupy a řádů jejích podgrup?
$|G| = [G:H] \cdot |H|$; řád podgrupy dělí řád grupy
–Definuj podgrupu a normální podgrupu.
podgrupa = množina H tž: $\emptyset \neq H \subseteq G$, uzavřená na $\cdot$, $\forall h \in H : h^{-1} \in H$
normální podgrupa = podgrupa H grupy G tž: $\forall g \in G \forall h \in H : g \cdot h \cdot g^{-1} \in H$
–Definuj normální podgrupu a homomorfismus grup.
normální podgrupa = podgrupa H grupy G tž: $\forall g \in G \forall h \in H : g \cdot h \cdot g^{-1} \in H$
homomorf. grup = zobr. $f : G \to H$ slučitelné s jejich bin. operacemi
–Uveď df faktorové grupy (včetně značení a definice operací).
$G/\rho(\odot)$, na množině G/ρ definována operace $\odot$ tž $[a]_\rho \odot [b]_\rho = [a \cdot b]_\rho$, kde $G(\cdot)$ grupa, ρ ekvivalence na G sluč. s $\cdot$
–Uveď v. o homomorfismu pro grupy.
$f : G_1 \to G_2$ homomorf. grup, H je norm. podgrupa $G_1(\cdot)$. Pak $\exists$ homomorf. $g : G_1/H \to G_2$ splňující $g\pi_H = f \Leftrightarrow H \subseteq \text{Ker } f$. Navíc, jestliže g existuje, je to izomorf. $\Leftrightarrow f$ je na a Ker $f = H$.
–Uveď 1. v. o izomorfismu pro grupy.
Nechť $f : G_1 \to G_2$ homomorf. grup. Pak $f(G_1)$ je podgrupa G_2 a $G_1/Kerf(\cdot) \cong f(G_1)()$.
–Uveď 2. v. o izomorfismu pro grupy.
$G(\cdot)$ grupa, H, K její norm. podgrupy. $H \subseteq K \Rightarrow K/H$ je norm. podgrupa grupy $G/H(\cdot)$ a $G/K(\cdot) \cong (G/H)/(K/H)(\cdot)$.
–Definuj relaci $rmodH$ pro danou podgrupu H.
$(a,b) \in rmodH \Leftrightarrow a \cdot b^{-1} \in H$.
–Kdy je relace $rmodH$ kongruence na grupě $G(\cdot)$?
kongruence = ekvivalence sluč. s $\cdot$
právě když $H = [1]_\rho$ je norm. podgrupa $G(\cdot)$ a $\rho = rmodH$)
–Popiš pomocí podgrup všechny ekvivalence slučitelné s grupovou operací.

–Najdi grupu $G(\cdot)$ a její podgrupu H, aby relace $rmodH$ nebyla slučitelná s $\cdot$.

–Existuje mezi každou dvojicí grup nějaký homomorfismus? Stručně zdůvodni.
Ano, f: A –> B, každá grupa obsahuje neutrální prvek (1 náleží B), pokud na něj zobrazíme všechny prvky z A, splníme slučitelnost
–Existuje nekonečná grupa, která obsahuje jen jednu normální podgrupu? Stručně zdůvodni.
Ne, každá grupa G(*) má alespoň dvě podgrupy: {1}(*) a G(*)

—5—
–Může mít komutativní grupa nekomutativní vlastní podgrupu? Ano - příklad, ne - zdůvodni.
ne - komutativita není ničím porušena
komutativita je vlastností operace, ta je v podgrupě stejná

–Může mít nekomutativní grupa komutativní vlastní podgrupu? Ano - příklad, ne - zdůvodni.
ano - $\mathbf{S}_4$??????????????
–Je grupa permutací $\mathbf{S}_3(\circ)$ komutativní? Stručně zdůvodni.
ne - $(12) \circ (23) = (123)$, $(23) \circ (12) = (132)$
–Je grupa sudých permutací $\mathbf{A}_4(\circ)$ komutativní? Stručně zdůvodni.
ne - ??????????????
–Je grupa sudých permutací $\mathbf{A}_3(\circ)$ komutativní? Stručně zdůvodni.
ano - ??????????????
–Je aditivní grupa $\mathbb{Z} \times \mathbb{Z}(+)$ komutativní? Stručně zdůvodni.
ano - sčítá se po složkách
–Je $\{0, 1, -1\}(\cdot)$ grupa? Stručně zdůvodni.
ne - 0 není neutr. prvek ($1 \cdot 0 \neq 1$); 1 neutr. $\Rightarrow$ 0 není invertibilní ($\nexists x 0 \cdot x = 1$ - to samé pro -1)
–Je $\{1, -1\}(\cdot)$ grupa? Stručně zdůvodni.
ano - asoc. OK, neutr. prvek: 1 ($1 \cdot 1 = 1, -1 \cdot 1 = 1 \cdot -1 = -1$), invertibilita ($1 \cdot 1 = 1, -1 \cdot (-1) = 1$)
–Tvoří matice s násobením grupu? Stručně zdůvodni.
ne - různé rozměry matic $\Rightarrow$ násobení není definováno nebo: obecné matice (neregulární) nemají inverz
–Tvoří všechny fce $\mathbb{R} \to \mathbb{R}$ se skládáním grupu? Stručně zdůvodni.
ne - nemusí existovat inverzní prvek (není-li fce prostá)
–Uveď všechny (až na izomorfismus) grupy prvočíselné velikosti p.
$\mathbb{Z}_p$
–Uveď všechny (až na izomorfismus) grupy velikosti 2,3,4,5,6.
$\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_5, \mathbf{S}_3, \mathbb{Z}_6$
–Napiš aspoň 3 neizomorfní 8-prvkové grupy.
$\mathbb{Z}_8, \mathbb{Z}_2 \times \mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
–Napiš aspoň 2 neizomorfní 9-prvkové grupy.
$\mathbb{Z}_9, \mathbb{Z}_3 \times \mathbb{Z}_3$
–Napiš aspoň 2 neizomorfní 10-prvkové grupy.
$\mathbb{Z}_{10}, D_4$ (dihedrální - otočení)
–Napiš aspoň 2 neizomorfní 24-prvkové grupy.
$\mathbb{Z}_{24}, \mathbb{Z}_6 \times \mathbb{Z}_4$
–Napiš aspoň 3 neizomorfní 12-prvkové grupy.
$\mathbb{Z}_{12}, \mathbb{Z}_2 \times \mathbb{Z}_6, \mathbf{A}_4$, Z2 x Z2 x Z3
–Rozhodni, zda iracionální čísla tvoří podgrupu grupy $\mathbb{C}(+)$. Stručně zdůvodni.

–Rozhodni, zda iracionální čísla tvoří podgrupu grupy $\mathbb{C}^*(\cdot)$. Stručně zdůvodni.

–Rozhodni, zda celá čísla tvoří podgrupu grupy $\mathbb{C}(+)$. Stručně zdůvodni.
Ano – podmnožina: ok, uzavřenost: ok, inverzy: ok, netrální prvek: 0 => OK
–Rozhodni, zda celá čísla tvoří podgrupu grupy $\mathbb{C}^*(\cdot)$. Stručně zdůvodni.
Ne – neplatí invertibilita: např. inverz 2 (tj. 1/2) není celé číslo
–Rozhodni, zda racionální čísla tvoří podgrupu grupy $\mathbb{R}(+)$. Stručně zdůvodni.
Ano – podmnožina: ok, uzavřenost: ok, inverzy: ok, neutr.: 0 => OK
–Rozhodni, zda kladná čísla tvoří podgrupu grupy $\mathbb{R}(+)$. Stručně zdůvodni.
Ne – není inverz např. pro 1 (tj. –1 není kladné)

–Rozhodni, zda kladná čísla tvoří podgrupu grupy $\mathbb{R}^*(\cdot)$. Stručně zdůvodni.
Ano – podmnožina: ok, uzavřenost: ok, inverzy: x –> 1/x, neutr.: 1 => OK

–Rozhodni, zda tvoří sudá celá čísla podgrupu grupy $\mathbb{Q}(+)$. Stručně zdůvodni.
Ano – podmnožina: ok, uzavřenost: ok, inverzy: x –> -x, neutr.: 0 => OK

–Rozhodni, zda tvoří sudá čísla podgrupu grupy $\mathbb{Q}^*(\cdot)$. Stručně zdůvodni.
Ne – neplatí invertibilita: např. inverz 2 (tj. 1/2) není sudé číslo

–Rozhodni, zda přirozená čísla tvoří podgrupu grupy $\mathbb{Q}(+)$. Stručně zdůvodni.
(za předpokladu, že 0 NENÍ přirozené číslo:) Ne – chybí neutrální prvek

–Rozhodni, zda permutace splňující $\pi^2 = id$ tvoří podgrupu grupy $\mathbf{S}_3(\circ)$.
Ne – není uzavřenost (1 2) o (2 3) = (1 2 3)

–Rozhodni, zda liché permutace tvoří podgrupu grupy $\mathbf{S}_n(\circ)$.
ne - lichá $\circ$ lichá = sudá

–Rozhodni, zda tvoří množina $\{1, 7\}$ podgrupu grupy $\mathbb{Z}_9^*(\cdot)$. Stručně zdůvodni.
ne - $7 \cdot 7 = 49 \equiv_9 4 \notin \{1, 7\}$

–Rozhodni, zda tvoří množina $\{1, 3\}$ podgrupu grupy $\mathbb{Z}_{10}^*(\cdot)$. Stručně zdůvodni.
ne - $3 \cdot 3 = 9 \notin \{1, 3\}$

–Rozhodni, zda tvoří množina $\{1, 2, 4, 5, 10\}$ podgrupu grupy $\mathbb{Z}_{11}^*(\cdot)$. Stručně zdůvodni.
ne - $5 \cdot 5 = 25 \equiv_{11} 3 \notin \{1, 2, 4, 5, 10\}$

–Rozhodni, zda tvoří množina $\{1, 3, 9\}$ podgrupu grupy $\mathbb{Z}_{13}^*(\cdot)$. Stručně zdůvodni.
ano - $\emptyset \neq \{1, 3, 9\} \subseteq \mathbb{Z}_{13}^*$, uzavřenost: $1 \cdot 1, 1 \cdot 3, 1 \cdot 9, 3 \cdot 3, 3 \cdot 9, 9 \cdot 9 \in \{1, 3, 9\}$, invertibilita: $1^{-1} = 1, 3^{-1} = 9, 9^{-1} = 3$

–Rozhodni, zda tvoří množina $\{1, 4, 7\}$ podgrupu grupy $\mathbb{Z}_9^*(\cdot)$. Stručně zdůvodni.
ano - $\emptyset \neq \{1, 4, 7\} \subseteq \mathbb{Z}_9^*$, uzavřenost: $1 \cdot 1, 1 \cdot 4, 1 \cdot 7, 4 \cdot 4, 4 \cdot 7, 7 \cdot 7 \in \{1, 4, 7\}$, invertibilita: $1^{-1} = 1, 4^{-1} = 7, 7^{-1} = 4$

–Rozhodni, zda tvoří množina $\{1, 5\}$ podgrupu grupy $\mathbb{Z}_{12}^*(\cdot)$. Stručně zdůvodni.
ano - $\emptyset \neq \{1, 5\} \subseteq \mathbb{Z}_{12}^*$, uzavřenost: $1 \cdot 1, 1 \cdot 5, (5 \cdot 5) \mod 12 \in \{1, 5\}$, invertibilita: $1^{-1} = 1, 5^{-1} = 5$

–Rozhodni, zda lichá čísla tvoří podgrupu grupy $\mathbb{Z}(+)$? Stručně zdůvodni.
ne - není uzavřená na operaci + (liché + liché $\neq$ liché)

–Napiš, jak vypadají všechny podgrupy grup $\mathbb{Z}_n(+)$.
pro k/n: $\mathbb{Z}_k$ Zn je cyklická – bude mít pouze cyklické podgrupy; pro každý dělitel "k" právě 1, a to isomorfní s Zk

–Napiš, jak vypadají všechny podgrupy grup $\mathbb{Z}(+)$.
podle Lagrange jiné podgrupy nemá
$n\mathbb{Z}$??????????????

–Rozhodni, zda diagonální matice tvoří podgrupu grupy $\mathbf{GL}_n(\mathbb{Q})(\cdot)$. Stručně zdůvodni. (pokud je nulová matice diagonální:) Ne – nulová matice má det = 0, tedy není podmnožinou GL...
ano - splněna uzavřenost i invertibilita

–Rozhodni, zda horní trojúhelníkové matice tvoří podgrupu grupy $\mathbf{GL}_n(\mathbb{Q})(\cdot)$. Stručně zdůvodni. (pokud je nulová matice horní trojúhelníkovou:) Ne – viz výše
(jinak:) ano - neutr. prvek: I_n, ?????????????????????? a pokud platí uzavřenost a invertibilita

–Rozhodni, zda dolní trojúhelníkové matice tvoří podgrupu grupy $\mathbf{GL}_n(\mathbb{Q})(\cdot)$. Stručně zdůvodni.

—6—
–Definuj cyklickou grupu.
grupa $G(\cdot)$ tž $\exists g \in G : \langle g \rangle = G$
–Uveď všechny (až na izomorfismus) cyklické grupy.
$G(\cdot)$ cyklická nekonečná $\Rightarrow G(\cdot) \cong \mathbb{Z}(+)$; $G(\cdot)$ cyklická konečná, $|G| = n \Rightarrow G(\cdot) \cong \mathbb{Z}_n(+)$
–Nechť $k \in \{1, \ldots, n\}$. Za jakých podmínek $\langle k \rangle = \mathbb{Z}_n$? Kolik podgrup řádu k má grupa $\mathbb{Z}_n$?
$NSD(k, n) = 1$
$k/n \to 1$ podgrupa, jinak žádná tj. # podgrup cyklické grupy řádu n = # dělitelů čísla n
–Kolik existuje podgrup konečné cyklické grupy?
dělitelů jejího řádu
–Kolik generátorů obsahuje konečná a kolik nekonečná cyklická grupa?
$G(\cdot)$ konečná cyklická $\Rightarrow |G| = n, G(\cdot) \cong \mathbb{Z}_n(+) \Rightarrow$ # generátorů $= \varphi(n)$
$G(\cdot)$ nekonečná cyklická $\Rightarrow G(\cdot) \cong \mathbb{Z}(+) = \langle 1 \rangle = \langle -1 \rangle \Rightarrow$ 2 generátory
–Stručně popište protokol RSA.
p, q různá prvočísla, $m = nsn(p-1, q-1), e < m, NSD(e, m) = 1, d < m, (ed) \bmod m = 1, n = p \cdot q$. veřejný klíč: (n, e), soukromý klíč: d. informaci $a \in \mathbb{Z}_n$ zašifrovat: $(a^e) \bmod n$, rozluštění: umocnit v $\mathbb{Z}_n(\cdot)$ exponentem d $((a^e)^d = a^{ed} = a)$
–Existují dvě neizomorfní cyklické grupy řádu 57894212? Stručně zdůvodni.
ne - $G(\cdot)$ cyklická konečná $\Rightarrow G(\cdot) \cong \mathbb{Z}_{57894212}$
–Existují dvě neizomorfní cyklické grupy řádu 2^{1000}? Stručně zdůvodni.
ne - $G(\cdot)$ cyklická konečná $\Rightarrow G(\cdot) \cong \mathbb{Z}_{2^{1000}}$
–Existují dvě neizomorfní nekonečné cyklické grupy? Stručně zdůvodni.
ne - $G(\cdot)$ cyklická nekonečná $\Rightarrow G(\cdot) \cong \mathbb{Z}$
–Existuje podgrupa či faktorová grupa cyklické grupy, která není cyklická? Stručně zdůvodněte.
ne - $g([g]_H)$ generátor cykl. $G(\cdot)$ (faktorgrupy $G/H(\cdot) \Rightarrow G(\cdot) \cong \mathbb{Z}(+)$, kde $|G| < \infty, G(\cdot) \cong \mathbb{Z}_n(+)$, kde $|G| = n \Rightarrow \mathbb{Z}(+)$ obsahuje jen podgrupy tvaru $n\mathbb{Z} = \langle n \rangle \Rightarrow G(\cdot)$ cyklická ...
–Obsahuje každá aspoň dvouprvková konečná grupa nějakou konečnou aspoň dvouprvkovou cyklickou podgrupu? Stručně zdůvodni.
ano - $G(\cdot)$ grupa, $g \in G$, $\langle g \rangle$ cyklická, za g zvolit prvek, který není v G neutrální $\Rightarrow |\langle g \rangle| \geq 2$
–Obsahuje každá nekonečná grupa nekonečnou cyklickou podgrupu? Stručně zdůvodni.
?????????????

—7—
–Uveď df algebry a podalgebry.
algebra = množina se systémem operací $(\alpha_i | i \in I)$
podalgebra = podmnožina nosné množiny algebry uzavřená na všechny operace z algebry
–Uveď df homomorfismu mezi algebrami $A(\alpha_i \mid i \in I)$ a $B(\alpha_i \mid i \in I)$.

zobr. $f : A \to B$ slučitelné s α_i $\forall i$, kde algebry jsou stejného typu
–Uveď df izomorfismu mezi algebrami $A(\alpha_i \mid i \in I)$ a $B(\alpha_i \mid i \in I)$.
bijektivní homomorfismus (homomorf. je zobr. slučitelné se všemi operacemi)
–Pro jaké algebry je prázdná množina podalgebrou?
?????????????????????????? pro ty, které nemají žádnou nulární operaci
–Co znamená, že množina X generuje algebru $A(\alpha_i \mid i \in I)$?
$\langle X \rangle = A$, kde $\langle X \rangle$ je nejmenší podalgebra algebry A obsahující množinu X
–Co znamená, že jsou algebry izomorfní? průnik všech podalgeber A obsahujících množinu X
existuje mezi nimi izomorfismus = bijektivní homomorf (homomorf. = zobr. slučitelné se všemi operacemi)
–Co znamená, že jsou algebry stejného typu?
operace jsou stejné arity
–Definuj uzávěrový systém.
množina $\mathcal{C} \subseteq \mathcal{P}(A)$, pokud $A \in \mathcal{C}$ a $\forall \{B_i | i \in I\} \subseteq \mathcal{C}$ je $\cap \{B_i | i \in I\} \in \mathcal{C}$
–Uveď aspoň tříprvkový příklad uzávěrového systému.
$\{1, 2, 3, 4\}, \{1, 2, 3\}, \{2, 3\}$
–Existuje vždy nějaký homomorfismus algebry do sebe? Stručně zdůvodni.
ano - id
–Existuje vždy nějaký izomorfismus algebry do sebe? Stručně zdůvodni.
ano - id
–Existuje mezi každou dvojicí algeber stejného typu nějaký homomorfismus? Stručně zdůvodni.
ne - ???????????
–Existuje nekonečná algebra obsahující jedinou podalgebru? Stručně zdůvodni.
ne ??????????????????

—8—
–Uveď df faktorové algebry (včetně značení a df operací).
$A(\alpha_i | i \in I)$ algebra, $\sim$ kongruence na A, $A/\sim$??????????????
–Definuj kongruenci na algebře. k-ární operaci α' definujeme: α([a1]~, ..., [ak]~) = [α(a1, ..., ak)]~
evkivalence na množině slučitelná se všemi operacemi této algebry
–Je průnik dvou kongruencí na algebře vždy kongruence? Stručně zdůvodni.
ano - reflexivita: $id \in \rho \cap \sigma \Rightarrow$ tranz., sym., slučitelnost ok
–Je sjednocení dvou kongruencí na algebře vždy kongruence? Stručně zdůvodni.
ne - $A = a \sim b, B = a \sim c, a \sim c \notin A \cup B$??????????????
–Definuj slučitelnost ekvivalence s n-ární operací. Je každá ekvivalence slučitelná s každou nulární operací?
A množina, α n-ární operace na A, $\forall a_1, \ldots, a_n, b_1, \ldots, b_n \in A(a_i, b_i) \in \rho, i = 1..n \Rightarrow (\alpha(a_1, \ldots, a_n), (b_1, \ldots, b_n)) \in \rho$
α
–Uveď v. o homomorfismu pro algebry.
$f : A \to B$ homomorf. dvou algeber stejného typu, ρ kongruence na A. Pak existuje homomorf. $g : A/\rho \to B$ tž $g\pi_\rho = f \Leftrightarrow \rho \subseteq kerf$. Navíc, pokud g existuje, je g izomorfismus $\Leftrightarrow f$ je na a $kerf = \rho$.

–Uveď 1. v. o izomorfismu pro algebry.
$f : A \to B$ homomorf. dvou algeber stejného typu. Pak $f(A)$ je podalgebra B a $A/kerf \cong f(A)$.
–Uveď 2. v. o izomorfismu pro algebry.
$\rho \subseteq \sigma$ kongruence na algebře $A \Rightarrow A/\sigma \cong (A/\rho)/(\sigma/\rho)$.
–Uveď příklady aspoň dvou kongruencí na desetiprvkové algebře.
$id, A \times A$
–Uveď příklady aspoň dvou kongruencí na nekonečné algebře.
$id, A \times A$
–Uveď příklad kongruence a podalgebry na algebře $A(\alpha_i \mid i \in I)$.
$id, A(\alpha_i | i \in I)$
–Existuje nekonečná algebra, na níž je pouze jedna kongruence? Stručně zdůvodni.
ne, vždy id a A x A
–Kolik existuje neizomorfních konečných algeber, na nichž je pouze jedna kongruence? Stručně zdůvodni.
0?????????

—12—
–Definuj těleso.
okruh R, jestliže všechny prvky z $R \setminus \{0\}$ invertibilní a 1 != 0
–Definuj okruh.
algebra $R(+, \cdot, -, 0, 1)$ tž $R(+)$ je komut. grupa s neutr. prvkem 0 a operací opačného prvku $-$, $R(\cdot)$ monoid s neutr. prvkem 1 a $\forall a, b, c \in R$ pak $a \cdot (b + c) = a \cdot b + a \cdot c, (a + b) \cdot c = a \cdot c + b \cdot c$
–Definuj pravý a levý ideál okruhu.
pravý ideál okruhu = množina $I \subseteq R$, kde $R(+, \cdot, -, 0, 1)$ okruh, I podgrupa grupy $R(+)$ a $\forall i \in I, r \in R\ i \cdot r \in I$
levý ideál okruhu = množina $I \subseteq R$, kde $R(+, \cdot, -, 0, 1)$ okruh, I podgrupa grupy $R(+)$ a $\forall i \in I, r \in R\ r \cdot i \in I$
–Definuj ideál okruhu.
množina, která je zároveň levým a pravým ideálem
–Charakterizuj, které okruhy jsou tělesa pomocí pojmu pravý a levý ideál.
R netriviální okruh: je těleso $\Leftrightarrow$ neobsahuje žádné vlastní pravé ideály $\Leftrightarrow$ neobsahuje žádné vlastní levé ideály
–Uveď příklad okruhu a nějakého jeho ideálu.
$\mathbb{R}(+, \cdot, -, 0, 1)$, $\{0\}, \mathbb{R}$
–Uveď příklad okruhu, který není tělesem.
okruh Z(+, *, –, 0, 1), má ideál např. 2Z => není tělesem
–Popiš vztah množiny kongruencí a ideálů okruhu.
jsou mezi nimi vzájemně inverzní bijekce: a(I) = rmod I, b(ro) = [0]ro
–Popiš všechny ideály okruhu celých čísel.
tvaru $k\mathbb{Z}$, kde $k < n$ je 0 nebo dělitel n
–Najdi aspoň tři kongruence na okruhu celých čísel.
id, Z x Z, mod 2

—13—
–Spočti hodnotu Eulerovy fce $\varphi(1200)$.
$\varphi(1200) = \varphi(2^4 \cdot 3 \cdot 5^2) = 2^3 \cdot 2 \cdot (4 \cdot 5) = 320$
–Spočti hodnotu Eulerovy fce $\varphi(1008)$.
$\varphi(1008) = \varphi(2^4 \cdot 3^2 \cdot 7) = 2^3 \cdot (2 \cdot 3) \cdot 6 = 288$
–Spočti hodnotu Eulerovy fce $\varphi(2250)$.
$\varphi(2250) = \varphi(2 \cdot 3^2 \cdot 5^3) = 1 \cdot (2 \cdot 3) \cdot (4 \cdot 5^2) = 600$
–Spočti hodnotu Eulerovy fce $\varphi(2310)$.
$\varphi(2310) = \varphi(2 \cdot 3 \cdot 5 \cdot 7 \cdot 11) = 1 \cdot 2 \cdot 4 \cdot 6 \cdot 10 = 480$
–Spočti 11^{-1} v monoidu $\mathbb{Z}_{24}(\cdot)$.
$24 = 11 \cdot 2 + 2, 11 = 2 \cdot 5 + 1$
$2 = 24 - 11 \cdot 2, 1 = 11 - 2 \cdot 5 = 11 - (24 - 11 \cdot 2) \cdot 5 = 11 \cdot 11 - 24 \cdot 5 \Rightarrow 11^{-1} = 11$
–Spočti 13^{-1} v monoidu $\mathbb{Z}_{19}(\cdot)$.
$19 = 13 \cdot 1 + 6, 13 = 6 \cdot 2 + 1$
$6 = 19 - 13 \cdot 1, 1 = 13 - 6 \cdot 2 = 13 - (19 - 13 \cdot 1) \cdot 2 = 13 \cdot 3 - 19 \cdot 2 \Rightarrow 13^{-1} = 3$
–Spočti 5^{-1} v monoidu $\mathbb{Z}_{22}(\cdot)$.
$22 = 5 \cdot 4 + 2, 5 = 2 \cdot 2 + 1$
$2 = 22 - 5 \cdot 4, 1 = 5 - 2 \cdot 2 = 5 - (22 - 5 \cdot 4) \cdot 2 = 5 \cdot 9 - 22 \cdot 2 \Rightarrow 5^{-1} = 9$
–Spočti 7^{-1} v monoidu $\mathbb{Z}_{23}(\cdot)$.
$23 = 7 \cdot 3 + 2, 7 = 2 \cdot 3 + 1$
$2 = 23 - 7 \cdot 3, 1 = 7 - 2 \cdot 3 = 7 - (23 - 7 \cdot 3) \cdot 3 = 7 \cdot 10 - 23 \cdot 3 \Rightarrow 7^{-1} = 10$
–Kolik invertibilních prvků obsahuje monoid $\mathbb{Z}_{888}(\cdot)$?
$\varphi(888) = \varphi(2^3 \cdot 3 \cdot 37) = 2^2 \cdot 2 \cdot 36 = 288$
–Kolik invertibilních prvků obsahuje monoid $\mathbb{Z}_{999}(\cdot)$?
$\varphi(999) = \varphi(3^3 \cdot 37) = (2 \cdot 3^2) \cdot 36 = 648$
–Kolik invertibilních prvků obsahuje monoid $\mathbb{Z}_{777}(\cdot)$?
$\varphi(777) = \varphi(3 \cdot 7 \cdot 37) = 2 \cdot 6 \cdot 36 = 432$
–Kolik generátorů obsahuje cyklická grupa řádu 870?
konečná cyklická $G(\cdot) \cong \mathbb{Z}_n(+) \Rightarrow \varphi(870) = \varphi(2 \cdot 3 \cdot 5 \cdot 29) = 1 \cdot 2 \cdot 4 \cdot 28 = 224$
–Kolik generátorů obsahuje cyklická grupa řádu 880?
konečná cyklická $G(\cdot) \cong \mathbb{Z}_n(+) \Rightarrow \varphi(880) = \varphi(2^4 \cdot 5 \cdot 11) = 2^3 \cdot 4 \cdot 10 = 320$
–Kolik generátorů obsahuje cyklická grupa řádu 1300?
konečná cyklická $G(\cdot) \cong \mathbb{Z}_n(+) \Rightarrow \varphi(1300) = \varphi(2^2 \cdot 5^2 \cdot 13) = 2^1 \cdot (4 \cdot 5^1) \cdot 12 = 480$