Algebra – Guričanov testík z 3. semestra

1. Platí v konecnom poli $(Z_p, +, .)$ identita $x^p = x$? (Identita znamena, ze uvedena rovnost plati pre vsetky $x \in Z_p$.)

☐ áno ☐ nie

Riešenie.
ANO, zdovodnenie asi take, ze pre nulu to plati a ostatne prvky tvoria multiplik. grupu s $p-1$ prvkami, ich rad deli $p-1$, preto $x^{p-1} = 1$, a teda $x^p = x$.

2. Ktore z nasledujucich tvrdeni su pravdive:

☐ Nech $(R, +, .)$ je komut. okruh s 1, nech $I \subseteq R$ je jeho ideal, nech $(S, \oplus, \odot)$ je okruh a nech $\varphi : R \to S$ je surjektivny homomorfizmus okruhov. Potom $I' = \varphi(I) = \{s \in S \mid \exists i \in I; i\varphi = s\}$ je idealom v okruhu $(S, \oplus, \odot)$.

☐ Nech $(R, +, .)$ je komut. okruh s 1, nech $I \subseteq R$ je jeho ideal, nech $(S, \oplus, \odot)$ je okruh a nech $\varphi : R \to S$ je injektivny homomorfizmus okruhov. Potom $I' = \varphi(I) = \{s \in S \mid \exists i \in I; i\varphi = s\}$ je idealom v okruhu $(S, \oplus, \odot)$.

Riešenie.
ufff
jak sa mi toto nechce parsovat
prve PLATI, rozpise sa definicia idealu (uzavrety na minus a nas. prvkom R), z toho, ze φ je hom. okruhov to vypadne
druhe NEPLATI, lebo I' nemusi byt uzavrety na nasobenie tymi prvkami S, na ktore sa nic z R nezobrazi, napr. zobrazime cele cisla do realnych, ale ideal sa nezobrazi na ideal

3. Nech F je pole. Nech α, β su algebraicke nad F. Implikacia $m_\alpha(x) = m_\beta(x) \Rightarrow F(\alpha) = F(\beta)$

☐ plati ☐ neplati

Riešenie.
NIE, ma tam byt $F(\alpha) \sim F(\beta)$ (sú izomorfné), zoberme si napr. (autor je Brano) $\sqrt[4]{2}$ a $i\sqrt[4]{2}$, oba maju min. polynom $x^4 - 2$, ale prisl. polia su rozne.

4. Nech $(A, +, .)$ je komutativny okruh s 1. Nech x je transcendentny nad A. Potom $A[x]$ je obor integrity. Tvrdenie:

☐ plati ☐ neplati

Riešenie.
NIE
A musi byt obor integrity, lebo prvky A patria aj do $A[x]$ a preto ak ma A delitele nuly, ma ich aj $A[x]$. Ked je A obor integrity, tak to uz (myslim) plati. Tak ma napada, to uz je druhy semester, kedy do algebry zacinam vidiet az po skuske… Sranda…

5. Tvrdenie: Pocet prvkov pola je bud nekonecno alebo prvocislo

☐ plati ☐ neplati

Riešenie.
NIE, bud nekonecno alebo mocnina prvocisla

6. Hovorime, ze $c \in F$ (F je pole) je prave k-nasobnym korenom polynomu $f \in F[x]$, ak $(x-c)^k$ deli f a $(x-c)^{k+1}$ uz nedeli f (v $F[x]$). Nech F je pole, $f \in F[x]$ je polynom. Ak $c \in F$ je prave k-nasobny koren f, tak c je prave $(k-1)$-nasobny koren Df.
☐ ano ☐ nie

Riešenie.
NIE.
$f(x) = (x-c)^k g(x)$, kde $(x-c) \not| \; g(x)$. Potom $f'(x) = (x-c)^k g'(x) + k(x-c)^{k-1} g(x)$, takze c je urcite aspon $k-1$ nasobny koren, nemusi vsak byt *prave*, lebo napr. nad Z_k je druhy clen rovny 0.

7. Sucin dvoch oborov integrity je obor integrity. Uvedene tvrdenie plati?
☐ ano ☐ nie

Riešenie.
NIE, presnejsie sucin dvoch netrivialnych oborov integrity nikdy nie je obor integrity – sucin nenulovych prvkov $[a,0]$ a $[0,b]$ je nulovy prvok sucinu $[a.0 = 0, 0.b = 0]$.

8. Moze mat konecny obor integrity vlastne[1] idealy?
☐ moze ☐ nemoze

Riešenie.
NIE
Konecny obor integrity je pole $\Rightarrow$ ked ideal obsahuje x, tak obsahuje kvoli uzaveru na nasobenie aj prvok xx^{-1}, (v poli mame inv. prvky), teda obs. 1, preto je rovny celemu polu.

9. Nech $(A,+,.)$ je komutativny okruh. Nech $M = \{a,b\} \subseteq A$. Najmensi ideal $I \subseteq A$ obsahujuci M (t.j. $M \subseteq I$) sa da vyjadrit ako $I = \{r_1 a + r_2 b \mid r_1, r_2 \in A\}$
☐ ano ☐ nie

Riešenie.
NIE, malo by tam byt $r_1, r_2 \in N$, protipriklad si vymyslite
Pozn.: Ako to tak po sebe citam, nepaci sa mi to. Tu bude pruser.

10. Nech je pole F_1 rozsirenim pola F. Nech $\alpha, \beta \in F_1$ su algebraicke nad F take, ze $m_\alpha(x)! = m_\beta(x)$. Potom $F(\alpha) \neq F(\beta)$.
☐ plati ☐ neplati

Riešenie.
NIE, napr. $\sqrt[3]{2}$ a $-\sqrt[3]{2}$ maju rozne min. polynomy, ale polia rovnake. Veta z prednasky je len implikacia (t.j. *ak* sa rovnaju polynomy, *tak* ...)

[1] v starsej verzii boli nevlastne, tie zrejme moze mat vsetko...

11. Nech $(A, +, .)$ je obor integrity s 1, nech x je transcendentny nad A. Plati tvrdenie: "Ak A je euklidovsky okruh, potom je aj $A[x]$ euklidovsky okruh."?
☐ ano ☐ nie

Riešenie.
NIE, ale teraz uz nepamatam preco

12. Nech I je vlastny ideal okruhu $(Z[x], +, .)$. Nech I je prvoideal. Je I maximalny ideal?
☐ ano ☐ nie

Riešenie.
NIE, teda nemusi, tiez nepamatam preco, ale z tohto (vraj) vyplyva riesenie predchadzajucej ulohy.

13. Cykly neparnej dlzky tvoria podgrupu grupy vsetkych permutacii danej mnoziny.
☐ ano ☐ nie

Riešenie.
preboha NIE, vsak to nie je ani uzavrete na skladanie...

14. Nech G je konecna grupa. Je pocet pravych tried rozkladu grupy G podla podgrupy H rovnaky ako pocet lavych tried rozkladu grupy G podla podgrupy H?
☐ ano ☐ nie

Riešenie.
ANO, a plati to aj v intuitivnej verzii pre nekonecne grupy (t.j. existuje bijekcia...), vyplyva to z eeee, jak sa to, tusim Lagrangeovej vety o tom, ze aj jednych, aj druhych je $|G|/|H|$.
Ako sa Hari vyjadril – na niektore z tych otazok je aj odpoved ANO. (Ja som si to potom na dalsej tipol a nebola to pravda... hm...)

15. Nech $f(x) = a_0 + a_1x + \ldots + a_nx^n \in Z[x]$, $n \geq 1$, $a_n \neq 0$. Nech $p, q \in Z$, $q \neq 0$, $nsd(p, q) = 1$. Potom $p/q \in Q$ je koren polynomu $f(x)$ prave vtedy, ked $p|a_0$ a $q|a_n$. Uvedene tvrdenie:
☐ plati ☐ neplati

Riešenie.
ANO, plati, dokaz – dosadime, vynasobime q^n, ked to deli jednu stranu, musi to delit aj druhu, ked to tam deli vsetky cleny okrem jedneho, tak to musi delit aj ten jeden.

16. Nech je permutacia φ sucin cyklov $\pi_1, \ldots, \pi_k$ (v uvedenom poradi). Potom rad permutacie φ je najmensi spolocny nasobok radov cyklov $\pi_1, \ldots, \pi_k$. Uvedene tvrdenie:
☐ plati ☐ neplati

Riešenie.
NIE, zacitujem Nanku: "chyba tam take kuzelne slovicko, ze *disjunktnych*"

17. Je q^n-prvkove pole (q je prvocislo) rozkladovym polom polynomu $f(x) = x^{q^n-1} - 1$?
☐ ano ☐ nie

Riešenie.
Nevedno preco ale vraj neplati... Jedine ze by to malo byt $f(x) = x^n - 1$ nad Z_q?

18. Ma 27-prvkove pole 9-prvkove podpole?
☐ ano ☐ nie

Riešenie.
NIE, lebo keby malo, v nom vieme najst 3-prvkove podpole, no a kedze pole je vekt. priestor nad svojim podpolom a na prednaske bola ta taka veticka, co neviem ako sa vola, s tym ze $[A : B] \cdot [B : C] = [A : C]$, podla nej by muselo 2 delit 3, co ale nedeli. (Dimenzia 9-prv. nad tym 3-prv. je 2, 27-prv. nad 3-prv. 3, preto dimenzia 27-prv. nad 9-prv. by musela byt 3/2...)

19. Nech $(A, \oplus_a, \odot_a)$, $(B, \oplus_b, \odot_b)$, $(C, \oplus_c, \odot_c)$, $(D, \oplus_d, \odot_d)$ su okruhy. Nech $(A \times B, \oplus_{a\times b}, \odot_{a\times b})$ je izomorfne s $(C \times D, \oplus_{c\times d}, \odot_{c\times d})$. Potom $(A, \oplus_a, \odot_a)$ je izomorfné s $(C, \oplus_c, \odot_c)$ a $(B, \oplus_b, \odot_b)$ s $(D, \oplus_d, \odot_d)$. Uvedene tvrdenie:
☐ plati ☐ neplati

Riešenie.
NIE
ani omylom
a ani keby tam bolo "... alebo A s D a B s C"
lebo staci zobrat $A = Z_2 \times Z_3$, $B = \{0\}$, $C = Z_2$, $D = Z_3$, pripadne podobny priklad, kde B nie je prazdna, ale Z_5 a D je $Z_3 \times Z_5$.

20. Nech $f(x), g(x) \in Z[x]$ su polynomy s celociselnymi koeficientami. Nech $h(x) = f(x)g(x)$ ma len parne koeficienty. Potom aspon jeden z polynomov $f(x)$, $g(x)$ ma vsetky koeficienty parne.
☐ plati ☐ neplati

Riešenie.
ANO
toto plati
a Hari zacal splietat nieco s Eisensteinovym kriteriom a podobne ti, co vedia, uz maju zjezene vlasy na hlave, pre ostatnych vysvetlenie: toto vam neda naozaj

21. Nech q je prvocislo, $m, n \in \{1, 2, \ldots\}$. Potom q^m-prvkove pole ma q^n-prvkove podpole prave vtedy, ked:
☐ $m \geq n$ ☐ $n|m$

Riešenie.
B, vysvetlenie vid 18.

22. Z okruhov $Z \times Z$ a Z_{17} nema netrivialne delitele nuly:
☐ prave jeden ☐ oba

Riešenie.
PRAVE JEDEN
Teda ZxZ ma – $[0, 7] \cdot [77, 0] = [0, 0]$, a Z_{17} nema, lebo 17 je prvocislo $\Rightarrow$ Z_17 je pole.

23. Nech G_1,G_2,G_3,G_4 su styri stvorprvkove grupy. Musia byt niektore dve z nich izomorfne?
☐ ano ☐ nie

Riešenie.
ANO
Lebo stvorprvkove grupy su az na izomorfizmus len dve, je to v knihe, skuste si napisat tabulky scitania.

24. Nech $(A, +, .)$ je obor integrity. Relacia $\doteq$ je relacia ekvivalencie. Je to kongruencia na A? (Kongruencia na okruhu znamena, ze ak $a \doteq b$ a $c \doteq d$, tak $a + c \doteq b + d$ a $ac \doteq bd$.)
☐ ano ☐ nie

Riešenie.
Spravna odpoved je NIE, lebo nemusi splnat ani jednu podmienku, lebo relacia ekvivalencie je len pohadzanie prvkov do skatuliek bez ohladu na vztahy medzi nimi a na to, aby to bola kongruencia, to musi prave splnat este nieco navyse. Takze: majme Z_7, relacia ekvivalencie – vsetko okrem 3 je ekviv. navzajom, 3 nie je s nicim, mame: $1 \doteq 5$ a $2 \doteq 4$, ale $1 + 2 \not\doteq 5 + 4$ a ani $2.5 \not\doteq 1.4$.

25. Nech $F = \{a + b.\sqrt[3]{2} \mid a, b \in Q\}$. Je F pole?
☐ ano ☐ nie

Riešenie.
NIE
pole je $G = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \mid a, b \in Q\}$

26. Nech $\varphi : R \to S$ a $\psi : R \to S'$ su dva surjektivne homomorfizmy (kde R, S, S' su okruhy). Nech $\mathrm{Ker}_\varphi = \mathrm{Ker}_\psi$. Potom S je izomorfny s S'.
☐ plati ☐ neplati

Riešenie.
S aj S' su izomorfne s faktorizaciou R podla Ker_φ, preto to PLATI

27. Nech $\varphi : R \to S$ je okruhovy homomorfizmus. Nech R ma neutralny prvok vzhladom na nasobenie 1_r. Potom S ma netralny prvok na nasobenie (oznacme ho 1_s) a plati $1_r\varphi = 1_s$. Uvedene tvrdenie:
☐ plati ☐ neplati

Riešenie.
NEPLATI
Zoberme napr. zobrazenie z Z_7 do $Z_7 \times Z_2$ take, ze $x\varphi = [x, 0]$, to je okruhovy homomorfizmus, ale $Z_7 \times Z_2$ nema jednotku.
Keby bol φ navyse surjektivny, tak by to platilo, lebo $\forall a_s \in S \exists b_r \in R; b_r\phi = a_s$ a potom je $a_s \odot_s (1_r\varphi) = (b_r\varphi) \odot_s (1_r\varphi) = (b_r \odot_r 1_r)\varphi = b_r\varphi = a_s$.
Alebo inymi slovami ak ma S jednotku, je nou urcite $1_r\varphi$, ibaze za podmienok zo zadania S ju nemusi mat.

28. Nech $(A, +, .)$ je okruh. Nech $a \in A$ nie je netrivialny delitel nuly. Nech $b, c \in A$. Potom implikacia $ab = ac \Rightarrow b = c$:
☐ plati ☐ neplati

Riešenie.
Intuicia hovori, ze PLATI, tak idem vymysliet preco. Keby $b \neq c$, tak z $ab = ac$ mame $a(b-c) = 0$ a teda a je delitel 0.
Ibaze by sme chceli byt detailisti. Lebo potom a este moze byt *trivialny* delitel nuly, cize nula a tvrdenie nam pekne-krasne neplati...

29. Majme polynom $f(x)$ nad polom F. Nech $\deg(f) \geq 1$. Polynom $f(x)$ ma v nejakom nadpoli pola F aspon jeden viacnasobny koren prave vtedy, ked $\deg(nsd(f(x), Df(x))) \geq 1$. Uvedene tvrdenie:
☐ plati len ak pridame predpoklad $\mathrm{char}(F) = \infty$ ☐ plati vzdy

Riešenie.
No pockat. NSD oboch je polynom max. stupna ktory ich deli. A ked $(x-c)^2$ deli $f(x)$, tak $(x-c)$ urcite deli $Df(x)$ (vid 6.) preto $(x-c)$ deli ich NSD, a preto ten je aspon stupna 1. Ak boli vsetky kroky dobre, tak to PLATI.

30. Nech $(A, +, .)$, $(B, \oplus, \odot)$ su dva okruhy a nech $\varphi : A \to B$ je homomorfizmus okruhov. Potom:
- Ak je $(A, +, .)$ OHI, je aj $(B, \oplus, \odot)$ OHI
- Ak je $(B, \oplus, \odot)$ OHI, je aj $(A, +, .)$ OHI
☐ neplati ani jedno ☐ plati aspon jedno

Riešenie.
Prve zjavne NEPLATI, podobny argument ako napr. v 27. (Teda ten isty homomorfizmus, A je OHI, B nie je.)
Druhe... eee... intuicia hovori, ze by mohlo platit... Ibaze ani ono NEPLATI, lebo napr. $A = Z_3 \times Z_4 \times Z_4$ nie je OHI (lebo $\{[0,0,0],[0,2,0],[0,0,2],[0,2,2]\}$ je ideal a nie je hlavny), $B = Z_3$ je OHI, lebo je to pole a $\varphi : [x, y, z]\varphi = x$ je homom. okruhov (dufam). V 1. pripade keby φ bolo surjektivne, tak by to asi platilo.

31. Nech S je podpriestor konecnorozmerneho euklid. priestoru (E, g). Nech $\alpha = \beta + \gamma$, $\beta \in S$, $\gamma \in S^{\perp}$. Zadefinujme zobrazenie $\varphi : E \to S$ tak, ze $\alpha\varphi = \beta$. Odpovedzte na otazky:
- je φ linearne zobrazenie?
- plati $J_\varphi \oplus O_\varphi = E$?

Riešenie.
sa mi uz nesce, ale snad oba ANO