Въпрос 1: (Напишете определението за група)
Отговор: Едно непразно множество G, снабдено с бинарна операция $*$ ($\forall a, b \in G : a * b \in G$) наричаме група, ако:
• Операцията $*$ е асоциативна ($\forall a, b, c \in G : (a * b) * c = a * (b * c)$).
• Съществува неутрален елемент относно операцията $*$ ($\exists e \in G \, \forall a \in G : a * e = e * a = a$).
• Всеки елемент на G е обратим ($\forall a \in G \, \exists b \in G : a * b = b * a = e$).

Въпрос 2: (Напишете определението за абелева група)
Отговор: Едно непразно множество G, снабдено с бинарна операция $*$ ($\forall a, b \in G : a * b \in G$) наричаме абелева група, ако:
• Операцията $*$ е асоциативна ($\forall a, b, c \in G : (a * b) * c = a * (b * c)$).
• Операцията $*$ е комутативна ($\forall a, b \in G : a * b = b * a$).
• Съществува неутрален елемент относно операцията $*$ ($\exists e \in G \, \forall a \in G : a * e = e * a = a$).
• Всеки елемент на G е обратим ($\forall a \in G \, \exists b \in G : a * b = b * a = e$).

Въпрос 3: (Дайте пример на абелева група)
Отговор: Примери за абелеви групи:
• Групата (Z, +) е безкрайна абелева група.
• Групата (Q, +) е безкрайна абелева група.
• Групата (R, +) е безкрайна абелева група.
• Групата (C, +) е безкрайна абелева група.

Въпрос 4: (Дайте пример на неабелева група)
Отговор: $GL_n(F) = \{A \in M_n(F) \mid \det A \neq 0\}$ при $n \geq 2$, където F е числово поле, което е фиксирано, а бинарната операция е умножение на матрици.

Въпрос 5: (Какво представлява симетричната група на едно множество)
Отговор: Нека Ω_n е множество. Със $S\Omega$ означаваме множеството от всички биекции $f : \Omega \to \Omega$. Ако $f, g \in S\Omega$, под произведение на f и g разбираме тяхната композиция, т.е. изображението $f \circ g : \Omega \to \Omega$, което действа по правилото $(f \circ g)(x) = f(g(x))$, $(x \in \Omega)$. С така въведената операция множеството $S\Omega$ се превръща в група.

Въпрос 6: (Напишете определението за пръстен)
Отговор: Нека R е множество, в което са дефинирани две бинарни операции - събиране (+) и умножение ($\cdot$) ($\forall a, b \in R : a + b \in R, a \cdot b \in R$). Казваме, че R е пръстен, ако R е абелева група относно операцията събиране и освен това за всеки три елемента $a, b, c \in R$ е изпълнено:
$(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (асоциативен закон)
$(a + b) \cdot c = a \cdot c + b \cdot c$ (дяснодистрибутивен закон)
$c \cdot (a + b) = c \cdot a + c \cdot b$ (ляводистрибутивен закон)

Въпрос 7: (Кога един пръстен е комутативен)
Отговор: Нека R е множество, в което са дефинирани две бинарни операции - събиране (+) и умножение (·) ($\forall$ a, b $\in$ R : a + b $\in$ R, a · b $\in$ R). Казваме, че R е комутативен пръстен, ако R е абелева група относно операцията събиране и освен това за всеки три елемента a, b, c $\in$ R е изпълнено:
(a · b) · c = a · (b · c) (асоциативен закон)
(a + b) · c = a · c + b · c (дяснодистрибутивен закон)
c · (a + b) = c · a + c · b (ляводистрибутивен закон)
a · b = b · a (комутативен закон)

Въпрос 8:(Кога един пръстен е с единица?)

Отговор: Нека R е множество, в което са дефинирани две бинарни операции – събиране (+) и умножение (·), т.е.

$\forall a,b \in R: a+b \in R, a \cdot b \in R$

Казваме, че R е **пръстен с единица**, ако:

- R е **абелева група** относно събирането;
- Съществува **неутрален елемент** относно умножението, наречен **единица** 1R, такъв че:

$\forall a \in R: a \cdot 1R = 1R \cdot a = a$

- Освен това за всички $a,b,c \in R$ са изпълнени:
    - $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ – асоциативен закон;
    - $(a+b) \cdot c = a \cdot c + b \cdot c$ – дяснодистрибутивност;
    - $c \cdot (a+b) = c \cdot a + c \cdot b$ – ляводистрибутивност.

Въпрос 9:(Кога един пръстен има делители на нулата)

Отговор:
Нека R е **комутативен пръстен** и $a \in R$. Казваме, че a е **делител на нулата**, ако съществува **ненулев елемент** $b \in R$, b❷=0R, такъв че:

$a \cdot b = 0R$ или $b \cdot a = 0R$

Тогава казваме, че в пръстена R **има делители на нулата**.

Въпрос 10:(Кога един пръстен е област на цялост)

Отговор:
Нека R е пръстен. Казваме, че R е **област на цялост**, ако са изпълнени следните условия:

- R❷={0},
- R е **комутативен пръстен**,

- В R **няма ненулеви делители на нулата**.

Въпрос 11:(Кога един пръстен е поле)

Отговор:
Нека R е непразно множество с дефинирани операции събиране (+) и умножение (·).
Казваме, че R е **поле**, ако:

- R е **комутативен пръстен с единица**, различна от нулата на пръстена;
- Всеки **ненулев елемент** на R е **обратим**, т.е.

$\forall a \in R,\ a \neq 0_R: \exists a^{-1} \in R: a \cdot a^{-1} = a^{-1} \cdot a = 1_R$

Въпрос 12:(Кога един пръстен е тяло)

Отговор:
Нека R е непразно множество с дефинирани операции събиране (+) и умножение (·).
Казваме, че R е **тяло**, ако:

- R е **пръстен с единица**, различна от нулата на пръстена;
- Всеки **ненулев елемент** на R е **обратим**, т.е. има мултипликативен обратен елемент.

Въпрос 13:(Напишете необходимо и достатъчно условие едно подмножество на един пръстен да е негов подпръстен)
Отговор:
Нека $(R,+,\cdot)$ е пръстен и $S \subseteq R$, $S \neq \varnothing$.
Необходимо и достатъчно условие S да бъде **подпръстен на R** е:

$\forall a,b \in S: a-b \in S и a \cdot b \in S$

Т.е. S трябва да е затворено относно изваждане и умножение.

Въпрос 14: (Напишете необходимо и достатъчно условие едно подмножество на едно поле да е негово подполе)
Отговор:
Нека $(F, +, \cdot)$ е поле и $K \subseteq F$, $K \neq \varnothing$. Необходимо и достатъчно условие

K да е подполе е за всеки два елемента $a, b \in K$ да следва, че $a - b,\ a \cdot b^{-1} \in K\ (b \neq 0)$.

Т.е. K трябва да е затворено относно изваждане и деление (без делене на нула).

Въпрос 15:(Какво е подгрупата породена от едно подмножество на дадена група)
Отговор:
Нека
G е група и $A \subseteq G$.

Подгрупа на G, породена от A, е **сечението на всички подгрупи на G**, съдържащи A.
Бележим с $\langle A\rangle$ и:

$$\langle A\rangle=\{a_1\varepsilon_1 a_2\varepsilon_2\ldots a_n\varepsilon_n \mid n\in N0;\ a_i\in A;\ \varepsilon_i=\pm1;\ i=1,\ldots,n\}$$

Въпрос 16:(Какво е подпръстена породен от едно подмножество на даден пръстен)
Отговор:
Нека
R е пръстен и $A\subseteq R$.
Подпръстен на R, породен от A, е **сечението на всички подпръстени на R**, съдържащи A.
Бележим с S[A] и:

$$S[A]=A\subseteq B\leq R\bigcap B=\{f(a_1,\ldots,a_n) \mid a_i\in A,\ 1\leq i\leq n\}=\{i=1\sum nj=1\prod m a_{ij}$$

Въпрос 17:(Какво е подполето породено от едно подмножество на дадено поле)
Отговор:
Нека
F е поле и $A\subseteq F$.
Подполето на F, породено от A, е **сечението на всички подполета на F**, съдържащи A.
Бележим с S(A) и:

$$S(A)=A\subseteq B\leq F\bigcap B=\{g(a_1,\ldots,a_n)f(a_1,\ldots,a_n)$$

Въпрос 18:(Кога едно изображение от една група в друга група е хомоморфизъм)
Отговор:
Нека са дадени групи $(G1, *1)$ и $(G2, *2)$ и $\varphi:G1\to G2$ е изображение.
Казваме, че φ е **хомоморфизъм на групи**, ако за всеки два елемента $a,b\in G1$ е изпълнено:

$$\varphi(a *1 b)=\varphi(a) *2 \varphi(b)$$

Въпрос 19:(Кога едно изображение от една група в друга група е изоморфизъм)
Отговор:
Нека са дадени групи $(G1, *1)$ и $(G2, *2)$ и $\varphi:G1\to G2$ е изображение.
Казваме, че φ е **изоморфизъм на групи**, ако за всеки два елемента $a,b\in G1$ е изпълнено:

$$\varphi(a *1 b)=\varphi(a) *2 \varphi(b)$$

и φ е **биекция**, т.е.:

- φ е инекция: $\forall a,b\in G1:\varphi(a)=\varphi(b)\Rightarrow a=b$
- φ е сюрекция: $\forall b\in G2\ \exists a\in G1:\varphi(a)=b$

Въпрос 20:(Кога едно изображение от един пръстен в друг е хомоморфизъм)
Отговор:
Нека са дадени пръстени $(R1,+1,\cdot1)$ и $(R2,+2,\cdot2)$ и $\varphi:R1\to R2$ е изображение.
Казваме, че φ е **хомоморфизъм на пръстени**, ако за всеки два елемента $a,b\in R1$ е изпълнено:

$\varphi(a+1b)=\varphi(a)+2\varphi(b), \varphi(a\cdot 1b)=\varphi(a)\cdot 2\varphi(b)$

Въпрос 21:(Кога едно изображение от един пръстен в друг е изоморфизъм)

Отговор:
Нека са дадени пръстени $(R1,+1,\cdot 1)$ и $(R2,+2,\cdot 2)$ и $\varphi: R1 \to R2$ е изображение.
Казваме, че φ е **изоморфизъм на пръстени**, ако за всеки два елемента $a,b \in R1$ е изпълнено:

$\varphi(a+1b)=\varphi(a)+2\varphi(b), \varphi(a\cdot 1b)=\varphi(a)\cdot 2\varphi(b)$

и φ е **биекция**, т.е.:

- φ е инекция: $\forall a,b \in R1: \varphi(a)=\varphi(b) \Rightarrow a=b$
- φ е сюрекция: $\forall b \in R2\ \exists a \in R1: \varphi(a)=b$

Въпрос 22:(Какво наричаме ядро на един хомоморфизъм на групи)

Отговор:
Нека $\varphi: G1 \to G2$ е хомоморфизъм на групи.
Множеството

$$Ker\varphi=\{a \in G1 \mid \varphi(a)=eG2\} \subseteq G1$$

наричаме **ядро на φ**.

Въпрос 23:(Какво наричаме ядро на един хомоморфизъм на пръстени)
Отговор:
Нека $\varphi: R1 \to R2$ е хомоморфизъм на пръстени.
Множеството

$$Ker\varphi=\{a \in R1 \mid \varphi(a)=0R2\} \subseteq R1$$

наричаме **ядро на φ**.

Въпрос 24:(Какво наричаме образ на един хомоморфизъм на групи)
Отговор:
Нека $\varphi: G1 \to G2$ е хомоморфизъм на групи.
Множеството

$$Im\varphi=\{b \in G2 \mid \exists a \in G1: \varphi(a)=b\} \subseteq G2$$

наричаме **образ на φ**.

Въпрос 25:(Какво наричаме образ на един хомоморфизъм на пръстени)
Отговор:

Нека $\varphi: R1 \to R2$ е хомоморфизъм на пръстени.
Множеството

$$Im\varphi = \{b \in R2 \mid \exists a \in R1 : \varphi(a) = b\} \subseteq R2$$

наричаме **образ на φ**.

Въпрос 26:(Какъв е образът на единичния елемент на една група при хомоморфизъм от нея в друга група)
Отговор:
Нека G1 и G2 са групи, а изображението $\varphi: G1 \to G2$ е хомоморфизъм на групи.
Тогава:

$$\varphi(eG1) = eG2$$

Въпрос 27:(Какъв е образът на нулевия елемент на един пръстен при хомоморфизъм от него в друг пръстен)
Отговор:
Нека R1 и R2 са пръстени, а изображението $\varphi: R1 \to R2$ е хомоморфизъм на пръстени.
Тогава:

$$\varphi(0R1) = 0R2$$

Въпрос 31: *Какво наричаме мултипликативна група на един пръстен?*
Отговор:
Нека R е пръстен с единица. С R^* означаваме множеството от всички обратими елементи на R. R^*, относно операцията умножение в пръстена, наричаме **мултипликативна група** на R.

Въпрос 32: *Какво наричаме адитивна група на един пръстен?*
Отговор:
Нека R е пръстен. С R+ означаваме абелевата група R относно операцията събиране в пръстена. Наричаме я **адитивна група** на R.

Въпрос 33:*Какво представлява мултипликативната група на пръстена от квадратните матрици с елементи от дадено поле?*
Отговор:
Нека Mn(F) е пръстенът от квадратни матрици с елементи от дадено поле F. Тогава $Mn(F)^*$ е групата GLn(F), която съдържа всички обратими квадратни матрици от ред n с елементи от F. Нарича се **обща линейна група** от ред n над полето F.

Въпрос 34: *Какво представлява мултипликативната група на пръстена на целите числа?*
Отговор:
Нека Z е пръстенът на целите числа. Тогава $Z^* = \{-1, 1\}$.

Въпрос 35: *Какво представлява мултипликативната група на поле?*
Отговор:
Нека F е поле. Тогава $F^* = F \setminus \{0\}$, тоест всички различни от нула елементи на F.

Въпрос 36:*Какво наричаме съседен клас на група по нейна подгрупа?*
Отговор:
Нека G е група, $H \leq G$, и $g \in G$. Множествата $gH = \{gh \mid h \in H\}$ и $Hg = \{hg \mid h \in H\}$ се наричат съответно **ляв** и **десен съседен клас** на G по подгрупата H.

Въпрос 37:*Какво е необходимо и достатъчно условие два елемента на една група да са в един и същ съседен клас на групата по дадена нейна подгрупа?*
Отговор:
Нека G е група, $H \leq G$, и $g_1, g_2 \in G$.

- Необходимо и достатъчно условие $g_1H = g_2H$ е $g_1^{-1}g_2 \in H$.
- Необходимо и достатъчно условие $Hg_1 = Hg_2$ е $g_2g_1^{-1} \in H$.

Въпрос 38:*Формулирайте теоремата на Лагранж.*
Отговор:
Нека G е крайна група и $H \leq G$. Тогава:

$$|G| = |H| \cdot |G:H|,$$

където $|G:H|$ е броят на левите (или десните) съседни класове на G по H.

Въпрос 39:*Напишете определението за нормална подгрупа на дадена група.*
Отговор:
Нека G е група и $H \leq G$. Казваме, че H е **нормална подгрупа** на G, ако за всеки $g \in G$ е изпълнено

$$gH = Hg.$$

Обозначаваме това с $H \trianglelefteq G$ или $H \trianglelefteq G$.

Въпрос 40:*Напишете необходимо и достатъчно условие една подгрупа на дадена група да е нормална.*
Отговор:
Необходимо и достатъчно условие $H \leq G$ да е **нормална подгрупа** на G е:
за всеки $g \in G$ и всеки $h \in H$ да е изпълнено

$ghg^{-1} \in H$.

Въпрос 41:*Какво наричаме факторгрупа?*
Отговор:
Нека G е група и $H \trianglelefteq G$. С G/H означаваме множеството от всички леви (или десни) съседни класове на G по H. Дефинираме бинарна операция в G/H така:

$aH \cdot bH = abH$.

Групата G/H, относно тази операция, се нарича **факторгрупа** на групата G по нормалната ѝ подгрупа H.

Въпрос 42:*Формулирайте теоремата за хомоморфизмите за групи.*
Отговор:
Нека G1 и G2 са групи и $\varphi: G1 \to G2$ е хомоморфизъм на групи. Нека $H = \ker\varphi$. Тогава $H \trianglelefteq G1$ и

$G1/H \cong \mathrm{Im}\varphi$.

Въпрос 43:*Какво наричаме идеал на даден пръстен?*
Отговор:
Нека R е пръстен и $I \subseteq R$ е подмножество на R. Казваме, че I е (двустранен) **идеал** на R, ако:

- за всякакви $a,b \in I$ е изпълнено $a - b \in I$;
- за всякакви $a \in I$ и $r \in R$ е изпълнено $ra \in I$ и $ar \in I$.
  Обозначаваме това с $I \trianglelefteq R$ или $I \triangleleft R$.

Въпрос 44:*Какво наричаме факторпръстен на даден пръстен по негов идеал?*
Отговор:
Нека R е пръстен и $I \trianglelefteq R$. С R/I означаваме множеството от всички леви (или десни) съседни класове на (R,+) по (I,+).
Дефинираме бинарните операции така:

$\bar{a} + \bar{b} = a + b, \bar{a} \cdot \bar{b} = ab$.

Тогава R/I с тези операции е **факторпръстен** на пръстена R по идеала I.

Въпрос 45:*Формулирайте теоремата за хомоморфизмите за пръстени.*
Отговор:
Нека R1 и R2 са пръстени и $\varphi: R1 \to R2$ е хомоморфизъм на пръстени. Нека $I = \ker\varphi$. Тогава $I \trianglelefteq R1$ и

$R1/I \cong \mathrm{Im}\varphi$.

Въпрос 46:*Напишете определението за ред на елемент на група.*
Отговор:

Нека G е група и $g \in G$. Най-малкото естествено число r, за което $gr=e$, се нарича **ред на елемента** g и се обозначава с r(g) или $|g|$.
Ако такова число не съществува, казваме, че g е от **безкраен ред** и пишем $r(g)=\infty$.

Въпрос 47:*Нека G е група и $g \in G$. Какво е необходимо и достатъчно условие $gk=eG$ за $k \in Z$?*
Отговор:
Необходимо и достатъчно условие $gk=eG$ е

$r(g) \mid k$.

Въпрос 48:*Нека G е група и $g \in G$. Какво е необходимо и достатъчно условие $gk=gl$ за $k,l \in Z$?*
Отговор:
Необходимо и достатъчно условие $gk=gl$ е

$k \equiv l (\mathrm{mod} r(g))$.

Въпрос 49:*Нека G е група и $g \in G$. Какъв е редът на елемента gk за $k \in Z$?*
Отговор:
Нека $r(g)=n$. Тогава

$r(gk)=\gcd(n,k)n$.

Въпрос 50:*Нека G е група и $g \in G$. Какво е необходимо и достатъчно условие редът на gk да е равен на реда на g, за $k \in Z$?*
Отговор:
Необходимо и достатъчно условие

$r(gk)=r(g)$

е

$\gcd(r(g),k)=1$.

Въпрос 51:
Напишете достатъчно условие редът на произведението на два комутиращи елемента на една крайна група да е равен на най-малкото общо кратно на редовете на тези елементи.
Отговор:
Нека G е крайна група, където $a,b \in G$ са комутиращи елементи. Достатъчно условие за

$|ab|=\mathrm{lcm}(|a|,|b|)$

е

$\langle a \rangle \cap \langle b \rangle = \{eG\}$.

Въпрос 52:
Напишете достатъчно условие редът на произведението на два комутиращи елемента на една крайна група да е равен на произведението на редовете на тези елементи.
Отговор:
Нека G е крайна група, където $a,b \in G$ са комутиращи елементи. Достатъчно условие за

$$| ab | = | a | \cdot | b |$$

е

$$\gcd(| a | , | b |)=1.$$

Въпрос 53:
Напишете определението за циклична група.
Отговор:
Нека G е група и $g \in G$. Подгрупата $\langle g \rangle$, породена от g и състояща се от всички степени на g, т.е.

$$\langle g \rangle = \{ g^n | n \in Z \}$$

(ако записът е адитивен, то $\langle g \rangle = \{ ng | n \in Z \}$), се нарича **циклична група**, породена от g, а g се нарича неин **пораждащ**.
Групата G е циклична, ако съществува $g \in G$, който поражда цялата група, т.е. $G = \langle g \rangle$.

Въпрос 54:
На коя група е изоморфна всяка крайна циклична група от ред n?
Отговор:
Всяка крайна циклична група от ред n е изоморфна на групата

$$C_n = \langle \omega 1 \rangle,$$

където $\omega 1$ е примитивен n-ти корен на единицата.

Въпрос 55:
На коя група е изоморфна всяка безкрайна циклична група?
Отговор:
Всяка безкрайна циклична група е изоморфна на адитивната група на целите числа Z.

Въпрос 56:
Нека елементът g поражда цикличната група G от ред n. Опишете всички пораждащи на групата G.
Отговор:
Нека $G = \langle g \rangle$ и $r(g)=n$. Тогава $G = \langle g^k \rangle$ точно тогава, когато

$$\gcd(k,n)=1.$$

Въпрос 57:
Нека елементът g поражда безкрайната циклична група G. Опишете всички пораждащи на групата G.
Отговор:
Нека $G=\langle g\rangle$ и $|G|=\infty$. Тогава $G=\langle gk\rangle$ точно тогава, когато $k=\pm 1$.

Въпрос 58:
Какви са подгрупите на циклична група?
Отговор:
Всяка подгрупа на циклична група също е циклична.

Въпрос 59:
Какви са редовете и пораждащите на подгрупите на безкрайна циклична група?
Отговор:
Нека $G=\langle g\rangle$, $|G|=\infty$. Всички подгрупи са или тривиалната $\{e\}=\langle e\rangle$, или $\langle gk\rangle=\langle g^{-k}\rangle$ за всяко $k \in N$. Редът на всяка неединична подгрупа е ∞.

Въпрос 60:
Какви са редовете и пораждащите на подгрупите на крайна циклична група?
Отговор:
Нека $G=\langle g\rangle$, $|G|=n$. Тогава подгрупа $H<G$ съществува точно когато има делител $d|n$ такъв, че

$H=\langle gd\rangle$,

и $|H|=dn$. За всеки такъв делител съществува точно една подгрупа с този ред. Всички пораждащи на $\langle gd\rangle$ са $\langle gdk\rangle$ за такива k, че

$gcd(k,dn)=1$.

Въпрос 61:
Какво е необходимо и достатъчно условие една подгрупа на дадена циклична група да е подгрупа на друга подгрупа на групата?
Отговор:
Нека G = hgi, т.е. G е крайна

циклична група. Необходимо и достатъчно условие за hg k i < hg l i < G е |hg k i| | |hg l i|. Знаем, че

r(g)

r(g)

r(g k) = (r(g),k)

и r(g l) = (r(g),l)

или l | k (l | k | |g|)

Въпрос 62. Формулирайте теоремата за делене с частно и остатък на две цели числа.

Отговор. За всяко две цели числа a и b, b❓=0, съществуват еднозначно определени цели числа q и r, такива че
a=bq+rи0≤r< | b | .

Въпрос 63. Какви са идеалите в пръстена на целите числа?

Отговор. Идеалите в пръстена на целите числа Z са главни и се описват като nZ, където $n \in N \cup \{0\}$.

Въпрос 64. Какво е необходимото и достатъчно условие един идеал да е подмножество на друг идеал в пръстена на целите числа?

Отговор. Нека (a),(b) ⊆ Z. Необходимо и достатъчно условие за (a) ⊆ (b) е да съществува $t \in Z$, такова че a=bt, т.е. b | a.

Въпрос 65. Кога две цели числа се делят взаимно?

Отговор. Нека $a,b \in Z$. Ако a | b и b | a, то b=±a. С други думи, (a)=(b) тогава и само тогава, когато b=±a.

Въпрос 66. Какво е необходимото и достатъчно условие d да поражда идеала, който е сума на идеалите породени от a и b в пръстена на целите числа?

Отговор. Нека $a,b,d \in Z$. Необходимо и достатъчно условие за (a)+(b)=(d) е:

- d | a и d | b;
- ако d0 | a и d0 | b, то d0 | d.

Въпрос 67. Какво е необходимото и достатъчно условие m да поражда идеала, който е

сечение на идеалите породени от a и b в пръстена на целите числа

Отговор. Нека a, b, m ∈ Z.

Необходимо и достатъчно условие (a) ∩ (b) = (m) е:

• a | m и b | m;

• ако a | m0 и b | m0 , то m | m0 .

Въпрос 68. Как се изразява идеалът породен от най-големия общ делител на две цели

числа в пръстена на целите числа чрез идеалите породени от тези числа

Отговор. Нека a, b ∈ Z. Тогава d = (a, b) поражда идеал (d) и за него е изпълнено (d) = (a) + (b).

Въпрос 69. Как се изразява идеалът породен от най-малкото общо кратно на две цели

числа в пръстена на целите числа чрез идеалите породени от тези числа) Нека

a, b ∈ Z. Тогава m = [a, b] поражда идеал (m) и за него е изпълнено (m) = (a) ∩ (b).

Въпрос 70. Формулирайте равенството на Безу за цели числа

Отговор. За всеки две числа a, b ∈ Z

съществуват числа u, v ∈ Z, такива че е изпълнено au + bv = (a, b).

Въпрос 71. Какво наричаме максимален идеал?

Отговор. Нека R е пръстен и I ⊆ R. Казваме, че I е максимален идеал, ако I❓=R и ако от I ⊆ J ⊆ R следва, че I=J или J=R.

Въпрос 72. Какво наричаме прост идеал?

Отговор. Нека R е пръстен и I ⊆ R. Казваме, че I е прост идеал, ако I❓=R и ако от ab ∈ I следва, че a ∈ I или b ∈ I.

Въпрос 73. Какво наричаме неразложим елемент в комутативен пръстен с единица?

Отговор. Нека R е комутативен пръстен с единица. Казваме, че a ∈ R е неразложим, ако a❓=0, a∈/R∗ (не е обратим) и от a=bc за b,c∈R следва, че b∈R∗ или c∈R∗.

Въпрос 74. Какво наричаме прост елемент в комутативен пръстен с единица?

Отговор. Нека R е комутативен пръстен с единица. Казваме, че a ∈ R е прост елемент, ако от a | bc следва, че a | b или a | c.

Въпрос 75. Какъв елемент е пораждащият на максимален идеал в област от главни идеали?

Отговор. Нека R е област на главни идеали и (a) ⊆ R е максимален идеал. Тогава елементът a е неразложим.

Въпрос 76. Какъв елемент е пораждащият на прост идеал в област от главни идеали?

Отговор. Нека R е област на главни идеали и (a) ⊆ R е прост идеал. Тогава елементът a е прост.

Въпрос 77. Какъв идеал е идеалът породен от неразложим елемент в област от главни идеали?

Отговор. Нека R е област от главни идеали и a ∈ R е неразложим елемент. Тогава идеалът (a) ⊆ R е максимален.

Въпрос 78. Какъв идеал е идеалът породен от прост елемент в област от главни идеали?

Отговор. Нека R е област от главни идеали и $a \in R$ е прост елемент. Тогава идеалът $(a) \subseteq R$ е прост.

Въпрос 79. За какъв идеал на комутативен пръстен с единица факторпръстенът е поле?

Отговор. Нека R е комутативен пръстен с единица. Ако $I \subseteq R$ и R/I е поле, то I е максимален идеал.

Въпрос 80. За какъв идеал на комутативен пръстен с единица факторпръстенът е област на цялост?

Отговор. Нека R е комутативен пръстен с единица. Ако $I \subseteq R$ и R/I е област, то I е прост идеал.

Въпрос 81. Какъв пръстен е факторпръстенът на комутативен пръстен с единица по максимален идеал?

Отговор. Нека R е комутативен пръстен с единица и $I \subseteq R$ е максимален идеал. Тогава факторпръстенът R/I е поле.

Въпрос 82. Какъв пръстен е факторпръстенът на комутативен пръстен с единица по прост идеал?

Отговор. Нека R е комутативен пръстен с единица и $I \subseteq R$ е прост идеал. Тогава факторпръстенът R/I е област на цялост.

Въпрос 83. Формулирайте основната теорема на аритметиката на целите числа.

Отговор. За всяко число $a \in Z$, $a \neq 0$, съществуват прости числа $p_1,\ldots,p_k$ и $\varepsilon = \pm 1$, които удовлетворяват следното:

$$a = \varepsilon \cdot p_1 \ldots p_k.$$

Това представяне на числото a е единствено с точност до реда на множителите.

Въпрос 84. Докажете, че съществуват безбройно много прости числа.

Отговор. Допускаме, че не съществуват безбройно много прости числа. Нека означим с $p_1, \ldots, p_k$ всички прости числа и разгледаме числото

$$P = p_1 p_2 \ldots p_k + 1.$$

Естественото число P се дели на някое просто число p, което трябва да е измежду $p_1,\ldots,p_k$. Но тогава $p \mid 1$, което е противоречие. Следователно има безбройно много прости числа.

Въпрос 85. Как се намира най-големият общ делител на две числа, ако са известни каноничните им разлагания на прости множители?

Отговор. Нека $a,b \in N$, като

$a=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k},\alpha_i \geq 0,$

и

$b=p_1^{\beta_1}p_2^{\beta_2}\ldots p_k^{\beta_k},\beta_i \geq 0.$

Тогава

$d=(a,b)=p_1^{\gamma_1}p_2^{\gamma_2}\ldots p_k^{\gamma_k},$

където

$\gamma_i=\min\{\alpha_i,\beta_i\},i=1,\ldots,k.$

Въпрос 86. Как се намира най-малкото общо кратно на две числа, ако са известни каноничните им разлагания на прости множители?

Отговор. Нека $a,b \in N$, като

$a=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k},\alpha_i \geq 0,$

и

$b=p_1^{\beta_1}p_2^{\beta_2}\ldots p_k^{\beta_k},\beta_i \geq 0.$

Тогава

$m=[a,b]=p_1^{\gamma_1}p_2^{\gamma_2}\ldots p_k^{\gamma_k},$

където

$\gamma_i=\max\{\alpha_i,\beta_i\},i=1,\ldots,k.$

Въпрос 87. Как се намира броят на положителните делители на естествено число, ако е известно каноничното му разлагане на прости множители?

Отговор. Нека $n \in N$ и

$n=p_1^{\beta_1}p_2^{\beta_2}\ldots p_k^{\beta_k},$

където $p_1,\ldots,p_k$ са различни прости числа, а $\beta_1,\ldots,\beta_k>0$. Тогава броят на положителните делители на числото n е

$(\beta_1+1)(\beta_2+1)\ldots(\beta_k+1).$

Въпрос 88. Как изглежда делител на естествено число, ако е известно каноничното му разлагане на прости множители?

Отговор. Нека $n \in N$ и

$n=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k},$

където $p_1,\ldots,p_k$ са различни прости числа, а $\alpha_1,\ldots,\alpha_k>0$. Тогава, ако $d \mid n$, то

$$d=p_1^{\beta_1}p_2^{\beta_2}\ldots p_k^{\beta_k},$$

където

$$0\leq\beta_i\leq\alpha_i, i=1,\ldots,k.$$

Въпрос 89. Какво представлява функцията на Ойлер?

Отговор. Нека n е естествено число. С $\varphi(n)$ бележим броя на естествените числа, ненадминаващи n и взаимно прости с n. Функцията $\varphi(n)$ се нарича функция на Ойлер.

Въпрос 90. Колко елемента има мултипликативната група на пръстена от класовете остатъци по модул n?

Отговор. Нека Z_n е пръстена на класовете остатъци по модул n. Тогава

$$|Z_n^*|=\varphi(n).$$

Въпрос 91. Кога един елемент на пръстена от класовете остатъци по модул n е обратим?

Отговор. Нека $\bar{a} \in Z_n$. Тогава $\bar{a}$ е обратим тогава и само тогава, когато $(a,n)=1$.

Въпрос 92. Кога един елемент на пръстена от класовете остатъци по модул n е делител на нулата?

Отговор. Нека $\bar{a} \in Z_n$. Тогава $\bar{a}$ е делител на нулата тогава и само тогава, когато $(a,n)\neq 1$.

Въпрос 93. Кога един елемент на пръстена от класовете остатъци по модул n не е обратим?

Отговор. Нека $\bar{a} \in Z_n$. Тогава $\bar{a}$ не е обратим тогава и само тогава, когато $(a,n)\neq 1$.

Въпрос 94. Кога един елемент на пръстена от класовете остатъци по модул n не е делител на нулата?

Отговор. Нека $\bar{a} \in Z_n$. Тогава $\bar{a}$ не е делител на нулата тогава и само тогава, когато $(a,n)=1$.

Въпрос 95. Формулирайте теоремата на Ойлер.

Отговор. Нека $n \in N$ и $r \in Z$, като $(r,n)=1$. Тогава

$$r^{\varphi(n)}\equiv 1 (\mathrm{mod} n).$$

Въпрос 96. Формулирайте теоремата на Ферма.

Отговор. Нека $r \in Z$ и p е просто число, като $p \nmid r$. Тогава

$r^{p-1} \equiv 1 \pmod{p}$.

Въпрос 97. Докажете, че редът на всяка подгрупа на крайна група дели реда на групата.
Отговор. Нека G е крайна група и H < G. От теоремата на Лагранж имаме, че |G| = |H|.|G : H|. Но $|G : H| \in \mathbb{Z}$. Тогава |H| | |G|.

Въпрос 98. Докажете, че индексът на крайна група по нейна подгрупа дели реда на групата.
Отговор. Нека G е крайна група и H < G. От теоремата на Лагранж имаме, че |G| = |H|.|G : H|. Но $|H| \in \mathbb{Z}$. Тогава |G : H| | |G|.

Въпрос 99. Докажете, че редът на произволен елемент на крайна група дели реда на групата.
Отговор. Нека G е крайна група и $g \in G$. Знаем, че r(g) = |hgi| = r, т.е. r е най-малкото естествено число, за което g^r = e. Нека H = hgi е цикличната подгрупа на G, породена от g. Тогава |H| = |hgi| = |g| = r. От теоремата на Лагранж имаме, че |G| = |H|.|G : H|. Но $|G : H| \in \mathbb{Z}$. Тогава |H| | |G|.

Въпрос 100. Докажете, че всеки елемент на крайна група на степен реда на групата дава единичния елемент на групата.
Отговор. Нека G е крайна група и $g \in G$. Нека r(g) = r, т.е. r е най-малкото естествено число, за което g^r = e. Нека H = hgi е цикличната подгрупа на G, породена от g. Тогава |H| = |hgi| = |g| = r. От теоремата на Лагранж имаме, че |G| = |H|.|G : H|. Но $|G : H| \in \mathbb{Z}$. Тогава |H| | |G|, т.е. r | |G|. Нека |G : H| = k. Получаваме, че g^|G| = g^{rk} = (g^r)^k = e^k = e.

Въпрос 101. Докажете, че всяка група от ред просто число е циклична.
Отговор. Нека G е крайна група от ред p, където p е просто число. Щом $|G| = p \geq 2$, то съществува елемент $g \in G$, такъв че $g \neq e$. hgi е цикличната група, породена от g. От теоремата на Лагранж следва, че |hgi| | |G| и тъй като p е просто число, а $g \neq e$, то следва, че |hgi| ≥ 2, а оттук |hgi| = p = |G|. Но hgi ≤ G, тоест достигаме до извода, че G = hgi, с други думи G е крайна циклична група от ред p, откъдето $G \cong C_p$.

Въпрос 102. Докажете, че всяка крайна група, която няма собствени подгрупи, е циклична от прост ред.
Отговор. Нека $G \neq \{e\}$ е крайна група, която няма собствени подгрупи, т.е. G няма подгрупи, различни от {e} и G. Нека $g \in G$ е такъв, че $g \neq e$. Тогава hgi ≤ G и $hgi \neq \{e\}$, откъдето следва, че hgi = G и G е циклична група. Групата G е крайна и тогава |G| = p за $p \in \mathbb{N}$. Знаем, че в този случай $G \cong C_p$. Ако p не е просто число, то съществува число $d \in \mathbb{N}$, $d \neq 1$, такова че d | p и $C_d \leq C_p$ е нетривиална подгрупа на C_p, което би означавало, че G също притежава нетривиални подгрупи. Стигнахме до противоречие, следователно числото p е просто.

Въпрос 103. Докажете теоремата на Ойлер.
Отговор. Ако елементите x, y ∈ Z, то x ≡ y (mod n) е еквивалентно на x̄ = ȳ в пръстена Zn. Тогава, ако изберем a ∈ Z, такова че (a, n) = 1, тогава ā е обратим в Zn, тоест ā ∈ Z ∗ n. От теоремата на Лагранж имаме, че ā^|Zn ∗ | = 1 или ā^ϕ(n) = 1̄, което е еквивалентно на a^ϕ(n) ≡ 1 (mod n).

Въпрос 104. Докажете теоремата на Ферма.
Отговор. Нека p ∈ Z. Ако елементите x, y ∈ Z, то x ≡ y (mod p) е еквивалентно на x̄ = ȳ в пръстена Zp. Тогава, ако изберем a ∈ Z, такова че (a, p) = 1, тогава ā е обратим в Zp, тоест ā ∈ Z ∗ p. От теоремата на Лагранж имаме, че ā^Zp = 1̄ или ā^ϕ(p) = 1̄, което е еквивалентно на a^ϕ(p) ≡ 1 (mod p) или a^{p−1} ≡ 1 (mod p). По-общо формулирано: a^p ≡ a (mod p), за всяко a ∈ Z.

Въпрос 105. Кога една числова функция е мултипликативна?
Отговор. Функцията f : N → C е мултипликативна, ако ∀ a, b ∈ N е изпълнено, че от (a, b) = 1 следва f(ab) = f(a)f(b).

Въпрос 106. Как се дефинира функцията на Мьобиус?
Отговор. Нека n е естествено число. Функцията

μ(n) =
1, ако n = 1,
0, ако n се дели на квадрат на просто число,
(−1)^s, ако n е произведение на s различни прости числа

се нарича функция на Мьобиус.

Въпрос 107
Ако с μ сме означили функцията на Мьобиус, на колко е равна сумата ∑_{d|n} μ(d) за естествено число n

Отговор
Нека M(n) = ∑_{d|n} μ(d). Тогава M(n) = 1 при n = 1 и M(n) = 0 при n > 1.

Въпрос 108
Формулирайте формулата за обръщане на Мьобиус

Отговор
Нека е дадена f : ℕ → ℕ и F(n) = ∑*{d|n} f(d), където n ∈ ℕ. Тогава е изпълнено, че* *f(n)* = ∑{d|n} F(d) μ(n/d) = ∑_{d|n} F(n/d) μ(d).

Въпрос 109
Ако с ϕ сме означили функцията на Ойлер, на колко е равна сумата ∑_{d|n} ϕ(d) за естествено число n

Отговор
Изпълнено е, че ∑_{d|n} ϕ(d) = n.

Въпрос 110
На колко е равна функцията на Ойлер за естествено число, ако е известно каноничното му разлагане на прости числа

Отговор
Нека $n \in \mathbb{N}$ и каноничното му разлагане на прости числа е $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. Тогава $\phi(n) = n \cdot (1 - 1/p_1) \dots (1 - 1/p_k)$.

Въпрос 111
Какво е необходимото и достатъчно условие едно линейно диофантово уравнение с две неизвестни да има решение

Отговор
Нека $a, b, c \in \mathbb{Z}$. Необходимо и достатъчно условие линейното диофантово уравнение $ax + by = c$ с две неизвестни x, y да има решение е $d = \gcd(a, b)$, $d \mid c$.

Въпрос 112
Как изглеждат всички решения на едно линейно диофантово уравнение с две неизвестни, ако е известно едно негово решение

Отговор
Нека $a, b, c \in \mathbb{Z}$. Ако (x_0, y_0) е решение на диофантовото уравнение $ax + by = c$ с неизвестни x, y, то всички решения са:
$x = x_0 - (b/d)\, t$,
$y = y_0 + (a/d)\, t$,
където $d = \gcd(a, b)$ и $t \in \mathbb{Z}$.

Въпрос 113
Какво е необходимото и достатъчно условие едно линейно сравнение с едно неизвестно да има решение

Отговор
Нека $a, b, c \in \mathbb{Z}$. Необходимо и достатъчно условие линейното сравнение $ax \equiv c \pmod b$ да има решение е $\gcd(a, b) \mid c$.

Въпрос 114
Как изглеждат всички решения на едно линейно сравнение с едно неизвестно, ако е известно едно негово решение

Отговор
Нека $a, b, c \in \mathbb{Z}$ и x_0 е едно решение на сравнението $ax \equiv c \pmod b$. Тогава всички решения са:
$x = x_0 + t \cdot (b / \gcd(a, b))$,
където $t = 0, \dots, \gcd(a, b) - 1$.

Въпрос 115
Кога два идеала в комутативен пръстен с единица са взаимно прости

Отговор
Нека R е комутативен пръстен с единица и I, J $\subseteq$ R идеали. Идеалите I и J са взаимно прости, ако I + J = R.

Въпрос 116
Формулирайте китайската теорема за остатъците за два идеала в комутативен пръстен с единица

Отговор
Нека R е комутативен пръстен с единица и I, J $\subseteq$ R идеали, като I и J са взаимно прости. Тогава:
$R / (IJ) \cong (R / I) \times (R / J)$.

Въпрос 117
Формулирайте китайската теорема за остатъците за пръстена на целите числа

Отговор
Нека n_1, ..., n_k са две по две взаимно прости числа. Тогава китайската теорема за остатъците гласи, че:
$\mathbb{Z}\_\{n_1 \ldots n\_k\} \cong \mathbb{Z}\_\{n_1\} \times \ldots \times \mathbb{Z}\_\{n\_k\}$.

Въпрос 118
Коя пермутация наричаме цикъл

Отговор
Нека $\Omega\_n = \{1, 2, \ldots, n\}$. Нека i_1, i_2, ..., i_k са различни числа от Ω_n, а σ е пермутацията, действаща по правилото:
$\sigma(i_1) = i_2$, $\sigma(i_2) = i_3$, ..., $\sigma(i\_\{k-1\}) = i\_k$, $\sigma(i\_k) = i_1$, а всички останали числа от Ω_n остават на място под действието на σ. Такава пермутация наричаме цикъл, а числото k — дължина на цикъла.

Въпрос 119
Кои цикли наричаме независими

Отговор
Два цикъла (i_1 i_2 ... i_k) и (j_1 j_2 ... j_s) наричаме независими, ако
$\{ i_1, i_2, \ldots, i\_k \} \cap \{ j_1, j_2, \ldots, j\_s \} = \varnothing$.

Въпрос 120
Какъв е редът на произведението на два независими цикъла

Отговор
Редът на произведението на два независими цикъла е равен на най-малкото общо кратно от редовете на двата независими цикъла.

Въпрос 121: Комутират ли циклите

Отговор:
Два независими цикъла σ и τ комутират. В общия случай циклите, които не са независими, не комутират.

Въпрос 122
Комутират ли независимите цикли

Отговор
Независимите цикли комутират винаги.

Въпрос 123
Какво е сечението на цикличните групи, породени от независими цикли

Отговор
Нека σ, τ ∈ S_n са независими цикли. Тогава hσi ∩ hτi = {id}.

Въпрос 124
Какво се получава като спрегнем цикъл с произволна пермутация

Отговор
Нека σ ∈ S_n. Тогава за пермутацията τ = (i_1 ... i_k) е изпълнено, че στσ^{-1} = (σ(i_1) ... σ(i_k)).

Въпрос 125
Какво наричаме транспозиция

Отговор
Цикъл с дължина 2 наричаме транспозиция.

Въпрос 126
Всеки ли цикъл се представя като произведение на транспозиции

Отговор
Всеки цикъл се представя като произведение на транспозиции.

Въпрос 127
Всеки ли цикъл се представя като произведение на независими транспозиции

Отговор
НЕ, всеки цикъл се представя като произведение на транспозиции, но не и на независими транспозиции.

Въпрос 128
Ако идентитетът е представен като произведение на транспозиции, какво можем да кажем за броя им

Отговор
Ако идентитетът е представен като произведение на транспозиции, то броят им е четно число.

Въпрос 129
Какво наричаме знак на пермутация

Отговор
Нека σ ∈ S_n и σ = τ_1 ... τ_k, където τ_i са транспозиции, тогава sign σ = (−1)^k наричаме знак на пермутацията σ.

Въпрос 130
Какво представлява алтернативната група

Отговор
Множеството от всички четни пермутации е подгрупа на S_n и се нарича алтернативна група от степен n, като я бележим с A_n. Също така |A_n| = 1/2 · n!.

Въпрос 131: Кога казваме, че една група действа върху дадено множество?
Отговор: Нека G е група, а M е множество. Казваме, че G действа върху M, ако съществува изображение

$\Phi: G \times M \to M,$

което на всеки елемент $g \in G$ и на всеки елемент $m \in M$ съпоставя елемент $g \circ m \in M$, като се изпълняват следните условия:

1. $e \circ m = m, \forall m \in M$ (където e е единичният елемент на G);
2. $(g1g2) \circ m = g1 \circ (g2 \circ m), \forall g1, g2 \in G, m \in M.$

Въпрос 132: Какво е необходимо и достатъчно условие група да действа върху множество?
Отговор: Необходимо и достатъчно условие група G да действа върху множество M е да съществува хомоморфизъм

$\varphi: G \to SM,$

където SM е симетричната група на множеството M.

Въпрос 133: Какво наричаме стабилизатор на елемент на множество при действие на група?
Отговор: Нека G е група, която действа върху множество M. Стабилизатор на елемент $m \in M$ е множеството

$StG(m) = \{g \in G \mid g \circ m = m\}.$

Въпрос 134: Какво наричаме орбита на елемент на множество при действие на група?
Отговор: Орбитата на елемент $m \in M$ при действието на G е множеството

$OG(m) = \{g \circ m | g \in G\}.$

Въпрос 135: Какво наричаме дължина на орбита при действие на група върху множество?
Отговор: Това е броят на елементите в орбитата на даден елемент m:

$| OG(m) |.$

Въпрос 136: Как се изразява дължината на орбитата при действие на крайна група?
Отговор:

$| OG(m) | = | G:StG(m) |,$

т.е. дължината на орбитата е индексът на стабилизатора на m в G.

Въпрос 137: Кое действие на група върху множество наричаме спрягане?
Отговор: Когато G действа върху себе си по формулата

$g \circ m = gmg-1,$

това действие се нарича спрягане.

Въпрос 138: Какво представлява един клас спрегнати елементи?
Отговор: Класът спрегнати с елемент $m \in G$ е множеството

$$O(m)=\{gmg^{-1} \mid g \in G\}.$$

Въпрос 139: Какво наричаме централизатор на елемент на група?
Отговор: Централизаторът на елемент m е множеството

$$C(m)=\{g \in G \mid gm=mg\}.$$

Въпрос 140: Какво наричаме център на група?
Отговор: Центърът на група G е множеството

$$Z(G)=\{z \in G \mid \forall g \in G: zg=gz\}.$$

Въпрос 141: Каква е формулата за класовете?
Отговор:

$$|G| = |Z(G)| + i\sum |G:C(mi)|,$$

където mi са представители на различни неединични класове на спрегнатост.

Въпрос 142: Какво можем да кажем за центъра на p-група?
Отговор: Центърът на всяка p-група е нетривиален, т.е.

$$Z(G) \neq \{e\}.$$

Въпрос 143: Какво можем да кажем за група от ред квадрат на просто число?
Отговор: Всяка група с ред p^2, където p е просто, е абелева.

Въпрос 144: Формулирайте теоремата на Поанкаре.
Отговор: Нека G е крайна група, $H < G$ и $|G:H| = n$. Тогава съществува хомоморфизъм

$$\varphi: G \to S_n$$

с ядро N, което е сечението на всички спрегнати на H подгрупи, и:

- $N \triangleleft G$,
- $N \leq H$,
- $n \mid |G:N|$,
- $|G:N| \mid n!$.

Въпрос 145: Формулирайте теоремата на Кейли.
Отговор: Всяка крайна група от ред n е изоморфна на подгрупа на симетричната група Sn.

Въпрос 146: Какво наричаме пръстен от формални степенни редове на една променлива с коефициенти от даден пръстен?
Отговор: Нека R е пръстен. Пръстен от формални степенни редове на една променлива с коефициенти от R наричаме

$R[[x]]=\{a=(a0,a1,\ldots,an,\ldots) \mid ai \in R\}$

със следните операции:
Събиране: $(a+b)i=ai+bi$
Умножение: $(a\cdot b)k=\sum i=0kaibk-i=\sum j=0kak-jbj$

Въпрос 147: Какво наричаме пръстен от полиноми на една променлива с коефициенти от даден пръстен?
Отговор: Нека R е пръстен. Пръстен от полиноми на една променлива с коефициенти от R наричаме

такова, че $R[x]=\{a=(a0,a1,\ldots,an,\ldots) \mid ai \in R, \exists k$ такова, че $\forall n>k:an=0\}$

със следните операции:
Събиране: $(a+b)i=ai+bi$
Умножение: $(a\cdot b)k=\sum i=0kaibk-i=\sum j=0kak-jbj$

Въпрос 148: Кога два полинома са равни в алгебричен смисъл?
Отговор: Два полинома $a,b \in R[x]$ са равни в алгебричен смисъл, ако за всяко i е изпълнено $ai=bi$.

Въпрос 149: Кога два полинома са равни във функционален смисъл?
Отговор: Два полинома $a,b \in R[x]$ са равни във функционален смисъл, ако за всяко $r \in R$ е изпълнено $a(r)=b(r)$.

Въпрос 150: Дайте пример на полиноми, равни във функционален смисъл, но различни в алгебричен.
Отговор:

1. В $Zp[x]$, $xp-x$ е равен на 0 във функционален смисъл, защото за всяко $a \in Zp$ имаме $ap=a$, но не е равен на 0 в алгебричен смисъл.
2. В $K=\{0,1\}$, полиномите $x2+1$ и $x4+1$ са равни във функционален смисъл, но различни алгебрично.

Въпрос 151: Какво наричаме степен на полином?
Отговор: Нека $A[x]$ е пръстен от полиноми с коефициенти от A, и $f \in A[x]$.

- Ако f❷=0, тогава degf=max{i|fi❷=0}
- Ако f=0, тогава degf=−∞

Въпрос 152: Какво можем да кажем за степента на сумата на два полинома, ако знаем степените им?
Отговор: Нека f,g ∈ A[x]. Тогава

deg(f+g)≤max{degf,degg}

Въпрос 153: Какво можем да кажем за степента на произведението на два полинома с коефициенти от даден пръстен?
Отговор: Нека f,g ∈ A[x]. Тогава

deg(fg)≤degf+degg

Въпрос 154: Какво можем да кажем за степента на произведението на два полинома с коефициенти от област на цялост?
Отговор: Нека A е област на цялост и f,g ∈ A[x]. Тогава

deg(fg)=degf+degg

Въпрос 155: Какво наричаме корен на полином?
Отговор: Нека F е поле и f ∈ F[x], α ∈ F. Тогава α е корен на полинома f, ако f(α)=0.

Въпрос 156: Напишете необходимо и достатъчно условие елемент на пръстен да е корен на полином с коефициенти от този пръстен.
Отговор: Нека F е комутативен пръстен с единица, f ∈ F[x], α ∈ F. Тогава α е корен на f, ако

f=(x−α)·q

за някой q ∈ F[x]

Въпрос 157: Напишете достатъчно условие два полинома от степен, не надвишаваща n, да са равни в алгебричен смисъл.
Отговор: Нека R е поле и f,g ∈ R[x], с degf,degg≤n. Ако съществуват n+1 различни α1,…,αn+1 ∈ R, за които f(αi)=g(αi), тогава f=g в алгебричен смисъл.

Въпрос 158: Формулирайте принципа за сравняване на коефициентите.
Отговор: Нека K е област и g1,g2 ∈ K[x], degg1,degg2≤n. Ако съществуват n+1 различни α1 ,...,αn+1 ∈ K, за които g1(αi)=g2(αi), тогава g1=g2.

Въпрос 159: Какво наричаме характеристика на поле?
Отговор:

1. Нека F е поле. Ако $n \cdot 1_? = 0$ за всяко $n \in N$, тогава charF=0.
2. Ако съществува най-малко естествено число p, за което $p \cdot 1 = 0$, то charF=p.

Въпрос 160: Какво число може да бъде характеристиката на едно поле?
Отговор: Характеристиката на поле може да бъде или 0, или просто число.

Въпрос 161: Нека характеристиката на полето F е нула. Какво е необходимото и достатъчно условие $n \cdot a = 0$ за $a \in F$?
Отговор: Необходимото и достатъчно условие е n=0 или a=0.

Въпрос 162: Нека характеристиката на полето F е различна от нула. Какво е необходимото и достатъчно условие $n \cdot a = 0$ за $a \in F$?
Отговор: Нека charF=p. Необходимото и достатъчно условие е $p \mid n$ или a=0.

Въпрос 163: Нека характеристиката на полето F е нула. Изоморфен образ на кое поле е подполе на F?
Отговор: Подполето на F е изоморфно на полето Q (рационалните числа).

Въпрос 164: Нека характеристиката на полето F е различна от нула. Изоморфен образ на кое поле е подполе на F?
Отговор: Подполето на F е изоморфно на полето Zp, където p=charF е просто число.

Въпрос 165: Кое поле наричаме просто?
Отговор: Казваме, че едно поле P е просто, ако няма собствени (различни от P) подполета.

Въпрос 166: Изоморфно на кои полета може да бъде едно просто поле?
Отговор: Едно просто поле може да бъде изоморфно на Q или на Zp, където p е просто число.

Въпрос 167: Ако характеристиката на едно поле е нула, на кое поле е изоморфно простото му подполе?
Отговор: Простото подполе е изоморфно на Q.

Въпрос 168: Ако характеристиката на едно поле е различна от нула, на кое поле е изоморфно простото му подполе?
Отговор: Простото подполе е изоморфно на Zp, където p е характеристиката на полето.

Въпрос 169: Формулирайте теоремата за делене с частно и остатък на полиноми.
Отговор: Нека F е поле и $f,g \in F[x]$, $g_? = 0$. Тогава съществува **единствена** двойка полиноми $q,r \in F[x]$, такива че

f=gq+rиdegr<degg.

Въпрос 170: Какви са идеалите в пръстен от полиноми на една променлива с коефициенти от поле?
Отговор: Ако F е поле, то всеки идеал I в пръстена F[x] е **главен**, т.е. от вида (f) за някой $f \in F[x]$.

Въпрос 171: Какво е необходимото и достатъчно условие един идеал да е подмножество на друг идеал в пръстена от полиноми с коефициенти от поле?
Отговор: Нека F е поле и $f,g \in F[x]$. Необходимо и достатъчно условие

$(g) \subseteq (f)$

е това, че $f \mid g$ в $F[x]$.

Въпрос 172: Какво е необходимото и достатъчно условие два идеала да са равни в пръстена от полиноми на една променлива с коефициенти от поле?
Отговор: Нека F е поле и $f,g \in F[x]$. Тогава

$(f)=(g) \mid \quad f\ g$ и $g \mid f \Longleftrightarrow \exists c \in F^{*} : g=cf$.

Въпрос 173: Какво наричаме най-голям общ делител на два полинома с коефициенти от поле?
Отговор: Нека F е поле и $f,g \in F[x]$, поне единият от които е ненулев. Полином d е **най-голям общ делител (НОД)** на f и g, ако

$(d)=(f)+(g)=((f,g))$.

Въпрос 174: Какво наричаме най-малко общо кратно на два полинома с коефициенти от поле?
Отговор: Нека F е поле и $f,g \in F[x]$, като $f❷=0$, $g❷=0$. Полином k е **най-малко общо кратно (НОК)** на f и g, ако

$(k)=(f) \cap (g)=([f,g])$.

Въпрос 175: Какво е необходимо и достатъчно условие един полином да е най-голям общ делител на два полинома с коефициенти от поле?
Отговор: Нека F е поле и $f,g \in F[x]$. Полиномът d е НОД на f и g тогава и само тогава, когато:

- $d \mid f$, $d \mid g$;
- ако $d1 \mid f$, $d1 \mid g$, то $d1 \mid d$.

Въпрос 176: Какво е необходимо и достатъчно условие един полином да е най-малко общо кратно на два полинома с коефициенти от поле?
Отговор: Нека F е поле и $f,g \in F[x]$. Полиномът k е НОК на f и g тогава и само тогава, когато:

- $f \mid k$, $g \mid k$;
- ако $f \mid k1$, $g \mid k1$, то $k \mid k1$.

Въпрос 177: Напишете равенството на Безу за полиноми с коефициенти от поле.
Отговор: Нека F е поле и $f,g \in F[x]$. Тогава съществуват полиноми $u,v \in F[x]$, такива че

$uf+vg=(f,g)$.

Въпрос 178: Какво наричаме неразложим полином в пръстен от полиноми на една променлива с коефициенти от поле?
Отговор: Нека $f \in F[x]$, $degf>0$, където F е поле. Казваме, че f е **неразложим над F**, ако не може да се представи като произведение на два полинома от $F[x]$ с положителни степени, по-малки от $degf$.

Въпрос 179: Какво е необходимо и достатъчно условие един полином да е неразложим в пръстен от полиноми с коефициенти от поле?
Отговор: Нека F е поле и $f \in F[x]$. Тогава f е неразложим над F тогава и само тогава, когато факторпръстенът

$F[x]/(f(x))$

е **поле**.

Въпрос 180: Формулирайте основната теорема на аритметиката на полиномите с коефициенти от поле.
Отговор: Всеки неконстантен полином $f \in F[x]$ се представя (до умножение с ненулеви скалари) **еднозначно** като произведение на неразложими над F полиноми:

$f=p1…pk$.

Ако $f=p1…pk=q1…qs$ са две такива разлагания, то $k=s$ и след евентуално преномериране съществуват $ai \in F^*$, такива че $pi=aiqi$.

Въпрос 181: Формулирайте схемата на Хорнер.
Отговор: Нека $f=a0xn+…+an \in F[x]$, $g=x-\alpha \in F[x]$, където F е пръстен с единица. Нека

$f=gq+r,c\ degr<degg \Rightarrow r \in F$.

Ако $q=b0xn-1+…+bn-1$, тогава:

- $b0=a0$
- $b1=a1+\alpha b0$
- $b2=a2+\alpha b1$
- ...

- $b_{n-1}=a_{n-1}+\alpha b_{n-2}$
- $r=a_n+\alpha b_{n-1}$

Въпрос 182: Ако един полином с коефициенти от поле F е неразложим над F, посочете поле, изоморфно на разширение на F, в което той има корен.
Отговор: Ако $f \in F[x]$ е неразложим, то **полето F[x]/(f(x))** е изоморфно на разширение на F, в което f има корен.

Въпрос 183: Какво наричаме поле на разлагане на полином с коефициенти от поле?
Отговор: Нека $f \in F[x]$, $\deg f>0$, и L е разширение на F, което съдържа **всички корени на f**. Тогава **полето на разлагане** на f е **сечението на всички подполета на L**, които съдържат F и всички корени на f.

Въпрос 184: Напишете формулите на Виет.
Отговор: Нека F е поле, $f=a_0x^n+\ldots+a_n \in F[x]$, и нека $\alpha_1,\ldots,\alpha_n$ са корените на f в подходящо разширение на F. Тогава:

$\alpha_1+\ldots+\alpha_n=-a_0a_1$, $1\leq i<j\leq n\sum\alpha_i\alpha_j=a_0a_2$, ... $\alpha_1\alpha_2\ldots\alpha_n=(-1)^na_0a_n$.

Въпрос 185
Какво наричаме k-кратен корен на полином?

Отговор
Нека $f \in F[x]$, K е разширение на F и $\alpha \in K$. Казваме, че α е k-кратен корен на f ($k \geq 1$), ако

$f=(x-\alpha)^kg, g \in K[x], и g(\alpha)\neq 0$.

При $k = 1$ казваме, че α е прост корен на f, а при $k > 1$ — че е кратен корен на f.

Въпрос 186
Какво е необходимото и достатъчно условие елемент на поле с характеристика нула да е k-кратен корен на полином с коефициенти от това поле?

Отговор
Нека F е поле, като $\mathrm{char}F = 0$, $f \in F[x]$, K е разширение на F и $\alpha \in K$. Тогава α е k-кратен корен на f точно когато

$f(\alpha)=f'(\alpha)=\ldots=f^{(k-1)}(\alpha)=0 и f^{(k)}(\alpha)\neq 0$.

Въпрос 187
Какво е необходимото и достатъчно условие елемент на поле да е кратен корен на полином с коефициенти от това поле?

Отговор
Нека $f \in F[x]$. Тогава f има кратен корен α тогава и само тогава, когато

$f(\alpha)=f'(\alpha)=0$,

тоест има общ корен с производната си.

Въпрос 188
Какво наричаме пръстен от полиноми на n променливи с коефициенти от област?

Отговор
Нека A е област. Тогава пръстенът от полиноми на n променливи с коефициенти от A се дефинира индуктивно по следния начин:

$A[x1,...,xn]=(A[x1,...,xn-1])[xn]=...=A[x1][x2]\ldots[xn-1][xn]$.

Въпрос 189
Какво представлява лексикографската наредба?

Отговор
Нека F е пръстен и $F[x1,...,xn]$ е пръстенът на полиномите на n променливи, $n \in N$.
Нека $u,v \in F[x1,...,xn]$, като $u=ax1i1\ldots xnin, v=bx1j1\ldots xnjn$ са два неподобни едночлена ($a, b \in F, a \neq 0, b \neq 0$).
Казваме, че $u>v$, ако съществува естествено число $k \leq n$, такова че $i1=j1,...,ik-1=jk-1$, но $ik>jk$.

Въпрос 190
Формулирайте лемата за старшия едночлен за полиноми на n променливи с коефициенти от област.

Отговор
Нека A е област и $f,g \in A[x1,...,xn]$, $f\text{❓}=0$, $g\text{❓}=0$.
Тогава старшият едночлен на полинома fg е равен на произведението от старшите едночлени на f и g.

Въпрос 191
Какво наричаме симетричен полином?

Отговор
Нека A е пръстен и $f=f(x1,...,xn) \in A[x1,...,xn]$.
Казваме, че f е симетричен полином, ако за всяка пермутация σ от симетричната група Sn е изпълнено равенството:

$f(x1,...,xn)=f(x\sigma(1),...,x\sigma(n))$.

Въпрос 192
Кои полиноми наричаме елементарни симетрични полиноми?

Отговор
Елементарните симетрични полиноми на n променливи са следните симетрични полиноми:

$\sigma1=x1+x2+\ldots+xn$, $\sigma2=x1x2+x1x3+\ldots+xn-1xn$, $\sigma3=x1x2x3+x1x2x4+\ldots+xn-2xn-1xn$,

...

$\sigma_n = x_1 x_2 \ldots x_n$.

Въпрос 193
Формулирайте основната теорема за симетричните полиноми.

Отговор
Нека A е област и $f = f(x_1,\ldots,x_n) \in A[x_1,\ldots,x_n]$ е симетричен полином.
Тогава съществува единствен полином g на n променливи с коефициенти от A, такъв че

$f(x_1,\ldots,x_n) = g(\sigma_1,\ldots,\sigma_n)$.

Въпрос 194
Формулирайте следствието от основната теорема за симетричните полиноми.

Отговор
Нека F е поле, $f = a_0 x^n + \ldots + a_n \in F[x]$, и $\alpha_1,\ldots,\alpha_n$ са всички корени на f (лежащи в подходящо разширение на F).
Тогава, ако $h(x_1,\ldots,x_n) \in F[x_1,\ldots,x_n]$ е симетричен полином, то

$h(\alpha_1,\ldots,\alpha_n) \in F$.

Въпрос 195
Кои полиноми наричаме степенни сборове?

Отговор
Нека A е пръстен и $f \in A[x_1,\ldots,x_n]$, където $n \in \mathbb{N}$.
Тогава

$S_k = x_1^k + x_2^k + \ldots + x_n^k, k = 0,1,2,\ldots$

се нарича степенен сбор. По определение $S_0 = n$.

Въпрос 196
Напишете формулите на Нютон за връзката между елементарните симетрични полиноми и степенните сборове.

Отговор
Нека

$S_k = x_1^k + x_2^k + \ldots + x_n^k$,

където $n \in \mathbb{N}$ и $k = 0,1,2,\ldots$ е степенният сбор на n променливи,
а $\sigma_1,\ldots,\sigma_k$ са елементарните симетрични полиноми.
Тогава равенствата от вида

$S_k - \sigma_1 S_{k-1} + \sigma_2 S_{k-2} - \ldots + (-1)^{k-1}\sigma_{k-1} S_1 + (-1)^k k \sigma_k = 0$

се наричат формули на Нютон.

Въпрос 197
Кое поле наричаме алгебрически затворено?

Отговор
Ще казваме, че едно поле F е алгебрически затворено, ако всеки неконстантен полином с коефициенти от F има корен в F.

Въпрос 198
Какво е полето, ако всеки полином с коефициенти от него се разлага на линейни множители?

Отговор
Ако за полето F е изпълнено, че за всеки полином $f \in F[x]$ корените на f са от F, т.е. f се разлага в произведение на линейни множители, то полето F е алгебрически затворено.

Въпрос 199
На какви множители се разлага полином с коефициенти от алгебрически затворено поле над това поле?

Отговор
Нека F е поле и $f \in F[x]$. Тогава f се разлага на линейни множители с коефициенти от полето F над самото поле F.

Въпрос 200
Кои са неразложимите полиноми с коефициенти от поле, ако полето е алгебрически затворено?

Отговор
Нека F е поле, което е алгебрически затворено. Тогава неразложимите полиноми с коефициенти от полето F са полиномите от първа степен (линейни полиноми от F[x]).

Въпрос 201
Какво е полето, ако единствените неразложими полиноми с коефициенти от това поле са полиномите от първа степен?

Отговор
Полето F, в което единствените неразложими полиноми с коефициенти от F са полиномите от първа степен, е алгебрически затворено.

Въпрос 202
Какво е полето на разлагане на полином с коефициенти от алгебрически затворено поле?

Отговор
Нека F е алгебрически затворено поле. Тогава полето на разлагане на полином с коефициенти от F съвпада с F.

Въпрос 203
Формулирайте лемата на Гаус за полиноми с реални коефициенти.

Отговор
Всеки неконстантен полином с реални коефициенти има поне един комплексен корен.

Въпрос 204
Формулирайте теоремата на Даламбер.

Отговор
Полето на комплексните числа $\mathbb{C}$ е алгебрически затворено.

Въпрос 205
Кои са неразложимите полиноми над полето на комплексните числа?

Отговор
Неразложимите полиноми над полето на комплексните числа са полиномите от първа степен.

Въпрос 206
Кои са неразложимите полиноми над полето на реалните числа?

Отговор
Неразложимите полиноми над полето на реалните числа са полиномите от първа степен и полиномите от втора степен с отрицателна дискриминанта.

Въпрос 207
Напишете определението за примитивен полином.

Отговор
Нека $f=a0xn+\ldots+an \in Z[x]$. Казваме, че f е примитивен полином, ако най-големият общ делител на коефициентите му a0,...,an е равен на 1, т.е. коефициентите му са (в съвкупност) взаимно прости.

Въпрос 208
Как се представя полином с рационални коефициенти чрез примитивен полином?

Отговор
Ако $g \in Q[x]$, то g може да се представи във вида $g=qrf$, където $f \in Z[x]$ е примитивен полином, $r,q \in Z$.

Въпрос 209
Напишете необходимо и достатъчно условие един полином с цели коефициенти да е примитивен.

Отговор
Необходимо и достатъчно условие $f \in Z[x]$ да е примитивен полином е: за всяко просто число p полиномът $f \in Zp[x]$ е ненулев.

Въпрос 210
Формулирайте лемата на Гаус за полиноми с цели коефициенти.

Отговор
Произведение на два примитивни полинома също е примитивен полином.

Въпрос 211
Какво можем да кажем, ако произведението на примитивен полином с рационално число е полином с цели коефициенти?

Отговор
Нека $h \in Z[x]$ е примитивен полином, $c \in Q$ и $ch \in Z[x]$. Тогава $c \in Z$.

Въпрос 212
Напишете необходимо и достатъчно условие полином с цели коефициенти да е неразложим над полето на рационалните числа.

Отговор
Нека $f \in Z[x]$. Необходимо и достатъчно условие полиномът f да е неразложим над полето $\mathbb{Q}$ е да е неразложим над пръстена $\mathbb{Z}$.

Въпрос 213
Напишете необходимо и достатъчно условие полином с цели коефициенти да е неразложим над пръстена на целите числа.

Отговор
Нека $f \in Z[x]$. Необходимо и достатъчно условие полиномът $f(x)$ да е неразложим над пръстена на целите числа е полиномът $f(ax+b)$ да е неразложим над пръстена на целите числа, $a,b \in Z, a \neq 0$.
Забележка: Възможно тълкуване на този въпрос е да бъде приет като дуален на предишния, откъдето трябва да се посочи, че необходимото и достатъчно условие е полиномът да е неразложим над рационалните числа. Препоръчително е да се напише второто, а първото да се знае за задачи.

Въпрос 214
Напишете необходимо и достатъчно условие полином с цели коефициенти да е разложим над полето на рационалните числа.

Отговор
Нека $f \in Z[x]$. Необходимо и достатъчно условие полиномът f да е разложим над полето $\mathbb{Q}$ е да е разложим над пръстена $\mathbb{Z}$.

Въпрос 215
Напишете необходимо и достатъчно условие полином с цели коефициенти да е разложим над пръстена на целите числа.

Отговор
Нека $f \in Z[x]$. Необходимо и достатъчно условие полиномът f(x) да е разложим над пръстена на целите числа е полиномът f(ax+b) да е разложим над пръстена на целите числа, $a,b \in Z, a \neq 0$.
Забележка: Възможно тълкуване на този въпрос е да бъде приет като дуален на предишния, откъдето трябва да се посочи, че необходимото и достатъчно условие е полиномът да е разложим над рационалните числа. Препоръчително е да се напише второто, а първото да се знае за задачи.

Въпрос 216
Напишете необходимо и достатъчно условие едно рационално число да е корен на полином с цели коефициенти.

Отговор
Нека $f=\sum_{i=0}^{n} a_i x^i \in Z[x], a_n \neq 0, \alpha = \frac{q}{p}$, където $p,q \in Z, gcd(p,q)=1$. Необходимо и достатъчно условие числото α да е корен на полинома f е:

- $p \mid a_n$ и $q \mid a_0$;
- $\forall m \in Z: (p - mq) \mid f(m)$.

Въпрос 217
Формулирайте критерия на Айзенщайн.

Отговор
Нека $f=a_0x^n+\ldots+a_n \in Z[x]$ и съществува просто число p, удовлетворяващо следните условия:

- $p \nmid a_0$;
- $p \mid a_1,\ldots,a_n$;
- $p^2 \nmid a_n$.
  Тогава полиномът f е неразложим над $\mathbb{Q}$.

Въпрос 218
Формулирайте редукционния критерий.

Отговор
Нека f=a0xn+…+an ∈ Z[x]. Ако p е просто число, което не дели a0, и редукционният полином f(x) ∈ Zp[x] е неразложим над Zp, то f(x) е неразложим над ℚ.

Въпрос 219: (Какъв може да е броят на елементите на крайно поле)
Отговор: Нека F е крайно поле и charF = p. Тогава |F| = p^n за някое естествено число n.

Въпрос 220: (Какво е необходимото и достатъчно условие за дадено естествено число да съществува крайно поле, чийто брой на елементите е това число)
Отговор: Нека n ∈ N. Необходимо и достатъчно условие да съществува поле F, за което |F| = n е числото n да е степен на просто число.

Въпрос 221: (Колко крайни полета с фиксиран брой елементи съществуват с точност до изоморфизъм)
Отговор: За всяко просто число p и за всяко число k ∈ N съществува единствено с точност до изоморфизъм поле с p^k елемента.

Въпрос 222: (Каква е мултипликативната група на крайно поле)
Отговор: Мултипликативната група на всяко крайно поле е циклична.

Въпрос 223: (Какво е необходимото и достатъчно условие едно крайно поле да е подполе на друго крайно поле)
Отговор: Нека F е крайно поле и K е също крайно поле, за които е изпълнено, че |F| = p^n и |K| = q^m, за p, q - прости числа и n, m ∈ N. Необходимо и достатъчно условие за K < F е charK = charF, т.е. p = q и m | n.

Въпрос 224: (Напишете определението за циклотомичен полином)
Отговор: Нека ζ_1, ..., ζ_φ(n) са примитивните n-ти корени на единицата. Полиномът Φ_n = Φ_n(x) = ∏_{k=1}^{φ(n)} (x − ζ_k) ∈ C ще наричаме n-ти циклотомичен полином.

Въпрос 225: (Как се представя полиномът x^n − 1 (за някое естествено число n), като произведение на циклотомични полиноми)
Отговор: За всяко естествено число n е в сила равенството x^n − 1 = ∏_{d|n} Φ_d, където произведението е взето по всички естествени делители на числото n.

Въпрос 226: (Как се изразява Φ_n (n ∈ N), чрез Φ_k за k = 1, ..., n − 1)
Отговор: Полиномът Φ_n се изразява по следния начин:
Φ_n = (x^n − 1) / ∏_{k|n, k<n} Φ_k.

Въпрос 227: (Какви числа са коефициентите на даден циклотомичен полином)
Отговор: За всяко естествено число n полиномът Φ_n е с цели коефициенти.

Въпрос 228: (Как се изразява циклотомичен полином, като се използва функцията на Мьобиус)
Отговор: За всяко естествено число n е в сила равенството Φ_n = ∏_{d|n} (x^d − 1)^{μ(d)}.

Въпрос 229: (Разложим или неразложим е даден циклотомичен полином над полето на рационалните числа)
Отговор: За всяко естествено число n полиномът Φ_n(x) е неразложим над полето Q.

Въпрос 230: (Разложим или неразложим е даден циклотомичен полином над пръстена на целите числа)
Отговор: За всяко естествено число n полиномът $\Phi_n(x)$ е неразложим над пръстена Z.

Въпрос 231: (Как се разлага на неразложими полиноми полиномът $x^n - 1$ (за някое естествено число n))
Отговор: Равенството $x^n - 1 = \prod_{d|n} \Phi_d(x)$ е разлагането на полинома $x^n - 1$ в произведение на неразложими над Q множители.

Въпрос 232: (Формулирайте теоремата на Ведербърн)
Отговор: Всяко крайно тяло е поле.