Matematiska Institutionen
KTH

Lösning till några övningar inför lappskrivning nummer 5, Diskret matematik för D2 och F, vt09.

1. Betrakat gruppen $G = (Z_{19} \setminus \{0\}, \cdot)$.

   (a) Visa att G är en cyklisk grupp.

   Lösning: Vi söker en generator till G, dvs ett element $g \in G$ sådant att varje element $h \in G$ är lika med en potens av g, dvs $h = g^k$ för något icke negativt heltal k. Detta element g måste ha ordning 18 eftersom $|G| = 18$, dvs $g^{18} = 1$ och ingen lägre exponent än 18 till g ger identitetselementet i G.

   Vi vet att ordningen av varje element är en delare till antalet element i G. Ett element i den givna gruppen har alltså någon av ordningarna 1, 2, 3, 6, 9 eller 18.

   Vi söker nu en generator g till givna gruppen med hjälp av trial and error.

   Prövar elementet 2. Vi testar om 2 har ordning 2, 3, 6 eller 9, vilka är de icke triviala delarna till talet 18.

   $$2^2 = 4 \neq 1, \quad 2^3 = 8 \neq 1, \quad 2^6 = 7 \neq 1, \qquad 2^9 = 2^3 \cdot 2^6 = 8 \cdot 7 = -1 \neq 1.$$

   Enda kvarvarande möjlighet för ordningen av elementet 2 är 18 och således är 2 en generator till gruppen G.

   Vår slutsats är alltså att eftersom G har ett element av ordning 18 och G består av 18 element så måste G vara cyklisk.

   (b) Bestäm antalet generatorer till G.

   Lösning: Det finns en sats i läroboken som säger att om G är en cyklisk grupp med n element så är antalet element av ordning d, där d delar n, lika med $\varphi(d)$, Eulers φ-funktion. Använder vi nu formeln

   $$\varphi(n) = n \cdot \Pi_{i=1}^{k}(1 - \frac{1}{p_i}) \qquad \text{om} \qquad n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k},$$

   där $p_1, p_2, \dots, p_k$ är olika primtal och exponenterna $e_i \geq 1$ för $i = 1, 2, \dots, k$, så får vi:
   SVAR:

   $$\varphi(18) = 18(1 - \frac{1}{2})(1 - \frac{1}{3}) = 6.$$

   (c) Bestäm delgrupper med 2, 3, 6 och 9 element till G.

   Lösning: Enligt samma sats i läroboken finns för varje delare d till 18 precis en delgrupp med d element. Dessutom vet vi att samtliga delgrupper till cykliska grupper är cykliska, och genereras alltså av element som har en ordning som är lika med antalet element i delgruppen. Om d delar n och elmentet g har ordning n så kommer $g^{n/d}$ att ha ordning d. Vi vet redan att elementet 2 har ordning 18 och finner då delgrupperna:

   $$H_2 = \{1, 2^9 = -1\}, \quad H_3 = \{1, 2^6 = 7, 2^{12} = 11\},$$

   $$H_6 = \{1, 2^3 = 8, 2^6 = 7, 2^9 = -1, 2^{12} = 11, 2^{15} = 12\},$$

   $$H_9 = \{1, 2^2 = 4, 2^4 = 16, 2^6 = 7, 2^8 = 9, 2^{10} = 17, 2^{12} = 11, 2^{14} = 6, 2^{16} = 5\}.$$

2. Bestäm antalet delgrupper till en cyklisk grupp med 63 element.

   Lösning: En cyklisk grupp G med n element har precis en delgrupp för varje delare d till n. För den givna gruppen G gäller att

   $$n = 63 = 7 \cdot 3^2,$$

   antalet delare blir då antalet möjliga sätt att kombinera potenser 7^e och 3^f, av talen 7 och 3, med $0 \leq e \leq 1$ och $0 \leq f \leq 2$. Vi får

   SVAR: $2 \cdot 3 = 6$.

3. Vilka av följande grupper är cykliska?

   (a) $(Z_2, +) \times (Z_3, +)$.

   Lösning: Elementet $(1, 1)$ genererar den direkta produkten ovan eftersom givna gruppen har sex element och elementet $(1, 1)$ varken har ordning 2 eller 3 eftersom

   $$2(1, 1) = (0, 1) =\neq (0, 0), \qquad \text{och} \quad 3(1, 1) = (1, 0) \neq (0, 0),$$

   och då ordningen av elementet $(1, 1)$ delar talet 6 så måste detta element ha ordning sex och alltså är givna gruppen cyklisk.

   (b) $(Z_8, +) \times (Z_9, +)$.

   Lösning: Elementet $(1, 1)$ genererar den direkta produkten ovan eftersom givna gruppen har 72 element och om elementet $(1, 1)$ har ordning k så måste

   $$k(1, 1) = (k, k) = (0, 0),$$

   vilket ger att 8 delar k och 9 delar k och alltså 72 delar k. Alltså har elementet $(1, 1)$ ordning 72 och den givna gruppen är cyklisk.

   (c) $(Z_8, +) \times (Z_3, +) \times (Z_3, +)$.

   Lösning: Låt (a, b, c) vara ett godtyckligt element i den givna gruppen. Då gäller, eftersom $a \in Z_8$, $b \in Z_3$ och $c \in Z_3$ att

   $$24(a, b, c) = (0, 0, 0),$$

   och alltså finns inget element som kan ha ordning 72, vilket var antalet element i gruppen.

4. Hörnen i en kvadrat färgas svarta eller vita. Kvadraten kan sedan speglas, vridas och vändas.

   (a) Bestäm en bana med precis två element, och en bana med precis fyra element.

   Lösning: Vi numrerar hörnen 1, 2, 3 och 4 så att hörn 1 har kant till hörn 4 och 2. Och kodar färgläggningarna så att 0 betyder vit färg och 1 svart färg, så tex $(0, 1, 1, 1)$ betecknar den färgläggning där hörn 1 är vitt och de övriga svarta.
   En bana med två element är då

   $$\{(0, 1, 0, 1), (1, 0, 1, 0)\},$$

   och en bana med fyra element är då t ex

   $$\{(0, 1, 1, 1), (1, 0, 1, 1), (1, 1, 0, 1), (1, 1, 1, 0)\}.$$

(b) Bestäm satibilisatorn till en färgläggning där två närliggande hörn är vita och de övriga två svarta.

Lösning: Vi betraktar färgläggningen $(0, 0, 1, 1)$. Stabilisatorn består av de vridningar, vändningar och speglingar som avbildar kvadraten på sig själv och så att färgläggningen bevaras. Identiteten, dvs ingen vridning etc alls är en sådan. Den enda andra möjligheten ges av att $1 \to 2$ och $2 \to 1$ och då måste även $3 \to 4$ och $4 \to 3$. Så
SVAR Med vår färgläggning blev stabilisatorn $\{id, (1\ 2)(3\ 4)\}$.

(c) Använd den sk Burnsides lemma för att beräkna antalet banor.

Lösning: Vi listar upp gruppen G av alla vridningar som avbildar kvadraten på sig själv och antalet färläggningar $|F(g)|$ som fixeras av respektive element $g \in G$:

G	$\lvert F(g)\rvert$
$id = (1)(2)(3)(4)$	$2^4 = 16$
$(1\ 2\ 3\ 4)$	2
$(1\ 3)(2\ 4)$	$2^2 = 4$
$(1\ 4\ 3\ 2)$	2
$(1)(3)(2\ 4)$	$2^3 = 8$
$(2)(4)(1\ 3)$	$2^3 = 8$
$(1\ 4)(2\ 3)$	$2^2 = 4$
$(1\ 2)(4\ 3)$	$2^2 = 4$

,

och alltså med Burnsides lemma
SVAR:

$$\frac{1}{|G|}\sum_{g\in G}|F(g)| = \frac{1}{8}(16 + 2\cdot 8 + 3\cdot 4 + 2\cdot 2) = \frac{48}{8} = 6.$$

Anmärkning: Motivering för att tabellen får de angivna värdena, se lösningen av nästa uppgift.

5. Bestäm antalet sätt att färga sidorna i en kub med 7 olika färger.

Lösning: Vi bestämmer först mängden vridningar av kuben som vrider kuben på sig själv, dvs kubens automorfigrupp.

Någon sida x skall vridas till kubens ovansida och någon av sidan x:s grannsidor y skall bli framsida. Antalet sätt att välja x är sex och då x har fyra angränsande sidor, finns det totalt $6 \cdot 4 = 24$ olika sätt att kombinera ihop x och y på så totalt finns det 24 automorfier av gruppen.

Vi skriver nu upp vår tabell, med beteckingar o=ovansida, b=baksida, f=framsida, u=undersida,h=högersida,v=vänstersida:

G	$\lvert F(g)\rvert$
$id = (v)(h)(f)(o)(b)(u)$	7^6
$(o)(u)(f\ v\ b\ h)$	7^3
$(o)(u)(f\ b)(v\ h)$	7^4
$(o)(u)(f\ h\ b\ v)$	7^3
nedan vrids f till o först	och sedan vrids kuben runt en tänkt z-axel
$(f\ o\ b\ u)(v)(h)$	7^3
$(f\ o\ h)(v\ b\ u)$	7^2
$(f\ o)(v\ h)(b\ u)$	7^3
$(f\ o; v)(b\ u\ h)$	7^2
nedan vrids v till o först	och sedan vrids kuben runt en tänkt z-axel ’
$(v\ o\ h\ u)(f)(b)$	7^3
$(v\ o\ f)(h\ u\ b)$	7^2
$(v\ o)(h\ u)(f\ b)$	7^3
$(v\ o\ b)(h\ u\ f)$	7^2
pss när b och h vrids till o först	och sedan vrids kuben runt en tänkt z-axel
$(o\ u)(f)(v)(b)(h)$	7^5
$(o\ u)(f\ v\ b\ h)$	7^2
$(o\ u)(f\ b)(v\ h)$	7^3
$(o\ u)(f\ h\ b\ v)$	7^2

och Burnsides lemma ger nu antalet banor

$$\frac{1}{|G|}\sum_{g\in G}|F(g)| = \frac{1}{24}(7^6 + 7^5 + 7^4 + 11\cdot 7^3 + 10\cdot 7^2) = 5880.$$

6. Undersök om polynomet $x^3 + x + 1$ är irreducibelt i polynomringen $Z_5[x]$.

   Lösning: Vore polynomet inte irreducibelt så skulle det, eftersom polynomets grad är tre, finnas faktorer av grad 1 och därmed enligt faktorsatsen skulle polynomet ha nollställen i kroppen Z_5. Detta är lätt att undersöka:

   $0^3{+}0{+}1 = 1 \neq 0,\ \ 1^3{+}1{+}1 = 3 \neq 0,\ \ 2^3{+}2{+}1 = 1 \neq 0,\ \ 3^3{+}3{+}1 = 1 \neq 0,\ \ 4^3{+}4{+}1 = 4 \neq 0.$

   Nollsällen saknas och polynomets grad är tre medför att polynomet är irreducibelt.

7. Undersök om polynomet $p(x) = x^4 + x^2 + 1$ är irreducibelt i polynomringen $Z_5[x]$.

   Lösning: Undersöker först om $p(x)$ har några så kallade linjära faktorer, dvs faktorer av grad 1, pss som i föregående uppgift.

   $0^4{+}0^2{+}1 = 1 \neq 0,\ 1^4{+}1^2{+}1 = 3 \neq 0,\ 2^4{+}2^2{+}1 = 1 \neq 0,\ 3^4{+}3^2{+}1 = 1 \neq 0,\ 4^4{+}4^2{+}1 = 2 \neq 0,$

   och alltså har polynomet inga linjära faktorer. Med hjälp av ansatsen

   $$x^4 + x^2 + 1 = (x^2 + Ax + B)(x^2 + Cx + D),$$

   undersöker vi nu förekomsten av andragradsfaktorer. Högra ledet förenklas till

   $$x^4 + (A + C)x^3 + (AC + B + D)x^2 + (BC + DA)x + BD,$$

och om vi sedan identierar koefficinter i $p(x)$ med koefficienterna i uttrycket ovan får vi systemet

$$\left\{\begin{array}{rcl} A+C & = & 0 \\ AC+B+D & = & 1 \\ BC+DA & = & 0 \\ BD & = & 1 \end{array}\right.$$

Multiplicerar vi första ekvationen med D och subtraherar den tredje ekvationen får vi likheten

$$(D-B)C = 0,$$

så om $D \neq B$ måste $C = 0$ och därmed också, i enlighet med ekvation 1, $A = 0$. Vi får två fall:

Fall 1: $D = B$ och emedan $DB = 1$ så finns i Z_5 bara möjligheterna $D = 1 = B$ och $D = B = -1$. Då får vi ur ekvation 1 och 2 att

$$\left\{\begin{array}{rcl} A+C & = & 0 \\ AC+2 & = & 1 \end{array}\right. \quad \text{resp} \quad \left\{\begin{array}{rcl} A+C & = & 0 \\ AC-2 & = & 1 \end{array}\right.$$

Men prövning med element ger med $A = 1$ och $C = 4$ att det första av dessa system är uppfyllt. Vi har då hittat en faktorisering:

$$x^4+x^2+1 = (x^2+1x+1)(x^2+4x+1),$$

och vårt systematiska sökande efter en faktorisering kan omdelbart avbrytas.

SVAR: Polynomet kan faktoriseras $x^4+x^2+1 = (x^2+x+1)(x^2+4x+1)$.

8. Betrakta polynomringen $Z_2[x]$ och bestäm den största gemensamma delaren $D(x)$ till de bägge polynomen $p(x) = x^5+x^3+x+1$ och $q(x) = x^2+1$ samt bestäm polynom $n(x)$ och $m(x)$ sådana att

$$D(x) = n(x)p(x) + m(x)q(x).$$

Lösning: Använder Euklides algoritm:

$$\begin{array}{rcl} x^5+x^3+x+1 & = & x^3(x^2+1)+x+1 \\ x^2+1 & = & (x+1)(x+1)+0 \end{array},$$

så $D(x) = (x+1)$. Vi finner också att

$$x+1 = (x^5+x^3+x+1) + x^3(x^2+1),$$

så

SVAR: $D(x) = x+1$ samt $n(x) = 1$ och $m(x) = x^3$ t ex.

9. Faktorisera polynomet x^6-1 i irreducibla faktorer i polynomringen

   (a) $Z_7[x]$.

   Lösning: Alla icke noll element i kroppen Z_7 satisfierar, pga Fermats lilla sats, ekvationen $x^6-1 = 0$. Vi har då faktoriseringen

$$x^6-1 = (x-1)(x-2)(x-3)(x-4)(x-5)(x-6).$$

(b) $Z_5[x]$.

Lösning: Undersöker först vilka av elementen i Z_5 som satisfierar ekvationen $x^6 = 1$. Vi finner att elementen 1 och -1 gör det och inga andra. Delar vi nu $x^6 - 1$ med polynomet $(x-1)(x+1)$ så får vi

$$x^6 - 1 = (x-1)(x+1)(x^4 + x^2 + 1).$$

Enligt en tidigare uppgift kan nu faktoriseringen fortsätta och vi finner att

$$x^6 - 1 = (x-1)(x+1)(x^2 + x + 1)(x^2 + 4x + 1).$$

(c) $Z_3[x]$.

Lösning: I Z_3 uppfyller alla icke noll element ekvationen $x^6 = 1$ och därför har vi som ovan

$$x^6 - 1 = (x-1)(x+1)(x^4 + x^2 + 1).$$

Även polynomet $x^4 + x^2 + 1$ har nollställena 1 och -1 och divison med $(x-1)(x+1)$ ger

$$x^4 + x^2 + 1 = (x-1)(x+1)(x^2 - 1).$$

Men $x^2 - 1$ har ju en välkänd faktorisering och vi får tillslut

$$x^6 - 1 = (x-1)(x+1)(x-1)(x+1)(x-1)(x+1).$$

(d) $Q[x]$.

Lösning: Vi löser först uppgift (e).

(e) $R[x]$.

Lösning: Vi löser först uppgift (e).

(f) $C[x]$,

Lösning: De komplexa rötterna till ekvationen äro $x_i = e^{i\frac{2\pi}{6}}$, där $x_0 = 1$ och $x_3 = -1$. Vi får nu faktoriseringen

$$x^6 - 1 = (x-1)(x+1)(x-x_1)(x-x_5)(x-x_2)(x-x_4).$$

Löser nu uppgifterna (d) och (e):
Rötterna x_1 och x_5 är konjugerade komplexa tal och produkten av motsvarande förstagrads ploynom blir $x^2 - x + 1$. Vi får nu faktoriseringen

$$x^6 - 1 = (x-1)(x+1)(x^2 - x + 1)(x^2 + x + 1)$$

och eftersom alla nollställen till andragradsfaktorerna ovan är ickereella så är en vidare faktorisering ej möjlig.

där Q betecknar kroppen av rationella tal, R kroppen av reellla tal och C de komplexa talen.

10. Visa att mängden

$$Z[\sqrt{2}] = \{n + m\sqrt{2} \mid n, m \in Z\},$$

där Z betecknar mängden av hela tal, bildar en ring.

Lösning: Den giva mängden är en delmängd till ringen av reella tal, där samtliga räknelagar för ringar är giltiga, så det enda vi behöver kontrollera är att den givna mängden är sluten

m a p addition och multiplikation samt att nollelement och additiva inverser till samtliga element existerar.

Vi testar nu slutenheten

$$(n_1 + m_1\sqrt{2}) + (n_2 + m_2\sqrt{2}) = (n_1 + n_2) + (m_1 + m_2)\sqrt{2} \in Z[\sqrt{2}],$$

eftersom $n_1 + n_2$ och $m_1 + m_2$ båda tillhör Z. Vidare är multiplikationen sluten ty

$$(n_1 + m_1\sqrt{2})(n_2 + m_2\sqrt{2}) = (n_1n_2 + 2m_1m_2) + (n_2m_1 + n_1m_2)\sqrt{2} \in Z[\sqrt{2}],$$

eftersom $n_1n_2 + 2m_1m_2$ och $n_2m_1 + n_1m_2$ båda är element i Z.

Nollelementet är $0 + 0\sqrt{2}$ och varje element $n + m\sqrt{2}$ har additiva inversen $-n - m\sqrt{2}$ ty summan av dessa element är ju 0.

---

11. Gruppen G är cyklisk och har en cyklisk delgrupp H med 105 element och en cyklisk delgrupp K med 63 element. Bestäm $H \cap K$.

Lösning: Vi observerar först att $sgd(105, 63) = 21$.

Eftersom H är cyklisk och talet 21 delar antalet element i H så finns precis en delgrupp L_H till H med 21 element. Motsvarande gäller för delgruppen K.

Nu använder vi Lagranges sats. Vi finner att antalet element i G delas av både 105 och 63 och alltså att talet 21 delar $|G|$. Eftersom G är cyklisk så har G precis en delgrupp L_G med 21 element. Men både L_H och L_K är också delgrupper till G, eftersom H och K är delgrupper till G, båda med 21 element. Enda möjligheten är att dessa grupper är lika, dvs

$$L_G = L_H = L_K.$$

Vi kan då sluta oss till att $L_G = L_H = L_K \subseteq K$ och $L_G = L_K = L_H \subseteq H$ och alltså

$$L_G \subseteq H \cap K.$$

Men $H \cap K$ delgrupp till både H och K ger att antalet element i $H \cap K$ delar antalet element i både H och K och alltså

$$|H \cap K| \mid sgd(105, 63) = 21.$$

Vi får alltså att $|H \cap K| \leq 21$. Men då $H \cap K$ innehåller en delgrupp L_G med 21 element så måste $|H \cap K| \geq 21$. Vi har nu kommit fram till att

$$21 \leq |H \cap K| \leq 21,$$

och alltså att

$$|H \cap K| = 21.$$

Men då $|L_G| = 21$ och $L_G \subseteq H \cap K$ så måste gälla att

$$H \cap K = L_G,$$

där L_G var den unika delgruppen till G med 21 element.

SVAR: $H \cap K$ är den unika delgruppen till G som har 21 element.

12. Betrakta en grupp G som verkar på en mängd S. Banan $\mathcal{O}$ innehåller 7 element ur S och stabilisatorn till elementet $s \in \mathcal{O}$ består av 4 element. Bestäm antalet element i G.

Lösning: Från den bakomliggande teorin för banor och sabilisatorer vet vi att, med bokens beteckningar, om H är stabilisatorn till s,

$$H = G(s \to s),$$

och s' ett annat element i samma bana, och g ett element i G sådant att $g(s) = s'$ så gäller att

$$G(s \to s') = gH.$$

Varje element i banan $\mathcal{O}$ motsvarar alltså en unik sidoklass till satbilisatorn H till $s \in \mathcal{O}$ (och H är ju en delgrupp till G).

Då H har fyra element och antalet sidoklasser är 7 så måste G innehålla precis 28 element.

SVAR: 28.

13. Låt H vara en delgrupp till gruppen G. Elementen i H beskriver funktioner på elementen i G enligt

$$h(g) = h \cdot g.$$

(a) Bestäm antalet banor i G.

Lösning: Vi använder Burnsides lemma och skall för den skull beräkna $|F(h)|$ för varje $h \in H$. Men i detta fall så är

$$F(h) = \{g \in G \mid hg = g\},$$

och alltså är $F(id) = G$ och om $h \neq id$ så gäller att $hg \neq g$ för varje $g \in G$ och således $F(h) = \emptyset$ om $h \neq id$. Enligt Burnsides lemma blir nu antal banor lika med

$$\frac{1}{|H|}\sum_{h\in H}|F(h)| = \frac{1}{|H|}|F(id)| = \frac{1}{|H|}|G| = \frac{|G|}{|H|}.$$

SVAR: Antalet banor är

$$\frac{|G|}{|H|}.$$

(b) Beskriv banorna.

Lösning: Låt Hg vara en sidoklass till H i G, dvs

$$Hg = \{hg \mid h \in H\}.$$

Då gäller för varje par av element hg resp $h'g$ i denna sidoklass att med $h'' = h'h^{-1} \in H$ så är

$$h''(hg) = h''hg = h'h^{-1}hg = h'g,$$

och därmed, enligt definitionen av bana, att hg och $h'g$ tillhör samma bana.

Nu räknar vi på antalet banor och antalet sidoklasser. Enligt uppgift (a) är antalet banor lika med $|G|/|H|$ vilket också är antalet sidoklasser. Eftersom elementen i en sidoklass tillhör samma bana, som vi visade ovan, så måste banorna bestå av sidoklasserna till H i G.

14. Undersök om mängden av 3×3 matriser

$$\begin{bmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{bmatrix},$$

där $a, b, c \in Z_5$, bildar en ring utan etta.

Lösning: Den giva mängden S är en delmängd till ringen av $R = M_{3\times 3}(Z_5)$ av 3×3-matriser med element från kroppen Z_5, där samtliga räknelagar för ringar är giltiga, så det enda vi behöver kontrollera är att den givna mängden är sluten m a p addition och multiplikation samt att nollelement och additiva inverser till samtliga element existerar.

Vi kontrollerar nu att matrisen är sluten m a p addition:

$$\begin{bmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & d & e \\ 0 & 0 & f \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & a+d & b+e \\ 0 & 0 & c+f \\ 0 & 0 & 0 \end{bmatrix} \in S.$$

Vidare med multiplikationen

$$\begin{bmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & d & e \\ 0 & 0 & f \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & af \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \in S.$$

Nollmatrisen fungerar som nollelement till mängden S och matrisen $-A$ är ju additiv invers till A i ringen R så det som återstår är att visa att $A \in S$ medför $-A \in S$:

$$A = \begin{bmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{bmatrix} \quad \Rightarrow \quad -A = \begin{bmatrix} 0 & -a & -b \\ 0 & 0 & -c \\ 0 & 0 & 0 \end{bmatrix} \in S.$$

15. Bestäm samtliga enheter i ringen $R = M_{2\times 2}(Z_2)$ av 2×2-matriser med element från kroppen Z_2.

Lösning: Vi definierar determinanter på sedvanligt sätt och räknelagen $\det(AB) = \det(A)\det(B)$ kommer att vara giltig. Så om A är en inverterbar matris finns en matris B sådan att

$$AB = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

och eftersom identitetsmatrisen kommer att ha en determinant som är lika med 1, så måste $\det(A) \neq 0$ om A är inverterbar. T ex genom att testa samtliga 16 matriser i den givna ringen ser man att ringen R består av 6 matriser med nollskild determinant:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}.$$

Vi prövar vidare och ser att de första fyra matriserna är sina egna inverser medan de två sista är varandras invers.

16. Betrakta ringen $R = M_{3\times 3}(Z_3)$ av 3×3-matriser med element från kroppen Z_3. Visa att om $A \in R$ och $\det(A) = 0$ så finns alltid en matris B sådan att $AB = 0$. Kommer det då också att finnas en matris C så att $CA = 0$?

Lösning: *Uppgiften blir trivial om vi tillåter B och C att vara nollmatriser. Så vi antar att det var icke nollmatriser som söktes!!* Vi vet från den linjära algebran att om determinanten för en matris A är noll så är kolonnerna linjärt beroende. Så om kolonnerna i A är $\bar{k}_1$, $\bar{k}_2$ och $\bar{k}_3$ så finns element λ_i, för $i = 1, 2, 3$ sådana att

$$\lambda_1\bar{k}_1 + \lambda_2\bar{k}_2 + \lambda_3\bar{k}_3 = \bar{0}.$$

Vanlig matrismutiplikation ger nu att med

$$B = \begin{bmatrix} \lambda_1 & \lambda_1 & \lambda_1 \\ \lambda_2 & \lambda_2 & \lambda_2 \\ \lambda_3 & \lambda_3 & \lambda_3 \end{bmatrix},$$

så blir $AB = 0$.

Eftersom $\det(A^T) = \det(A) = 0$ så finns en matris D till A^T sådan att $A^TD = 0$. Transponering i denna likhet ger nu att $D^TA = 0^T = 0$. De sökta matrisen C ges nu av matrisen $C = D^T$.

17. Polynomet $p(x) = x^5 - 3x^4 - 5x^3 + 15x^2 + 4x - 12$ har nollställena 1, -1, 2, -2 och 3 i ringen Z. Faktorisera $p(x)$ i irreducibla faktorer i ringen $Z_{17}[x]$.

Lösning: Faktoriseringen i ringen $R[x]$, där R är ett reellt tal blir ju, eftersom nollställena äro 1, -1, 2, -2 och 3,

$$x^5 - 3x^4 - 5x^3 + 15x^2 + 4x - 12 = (x-1)(x+1)(x-2)(x+2)(x-3).$$

Räknar vi nu modulo 17 så kommer samma likhet att bestå.

SVAR: $x^5 - 3x^4 - 5x^3 + 15x^2 + 4x - 12 = (x-1)(x+1)(x-2)(x+2)(x-3)$.

18. Konstruera ett irreducibelt fjärdegradspolynom i polynomringen $Z_3[x]$.

Lösning: Vi prövar oss fram och gör ett försök med polynomet

$$p(x) = x^4 + x + 2,$$

eftersom samtliga icke noll element a i Z_3 uppfyller $a^2 = 1$ och därmed $a^4 = 1$ så

$$a \neq 0 \;\Rightarrow\; a^4 + a + 2 = 1 + a + 2 = a \neq 0, \quad \text{och} \quad 04 + 0 + 2 = 2 \neq 0,$$

så polynomet vi prövar har inga förstagradsfaktorer.

Testar andragradsfaktorer genom en ansats:

$$x^4 + x + 2 = (x^2 + Ax + B)(x^2 + Cx + D),$$

Högra ledet förenklas till

$$x^4 + (A + C)x^3 + (AC + B + D)x^2 + (BC + DA)x + BD,$$

och om vi sedan identierar koefficinter i $p(x)$ med koefficienterna i uttrycket ovan får vi systemet

$$\begin{cases} A + C &= 0 \\ AC + B + D &= 0 \\ BC + DA &= 1 \\ BD &= 2 \end{cases}$$

eftersom Z_3 bara har tre element 0, 1 och 2 så ger den sista ekvationen att ett av elementen B och D är 1 och det andra 2 och då blir deras summa 0. Således ger ekvation 2 att $AC = 0$ varvid en av A och C måste vara noll, men eftersom summan av A och C är noll måste bägge elementen vara noll. Men då kan inte den tredje ekvationen vara uppfylld. Alltså finns inga andragradsfaktorer och polynomet är irrdeucibelt.

SVAR T ex polynomet $x^4 + x + 2$ är irreducibelt i $Z_3[x]$ och av grad fyra.

19. Bestäm antalet enheter i ringen $R = M_{2\times 2}(Z_p)$ av 2×2-matriser med element från kroppen Z_p, där p är ett primtal.

Lösning: Vi kan definiera determinanter i ringen R och ett element i denna ring är en enhet, dvs inverterbar, precis då dess determinant inte är noll. Totala antalet element i ringen R är p^4 eftersom Z_p innehåller p element och vi har att välja element till precis fyra positioner i varje matris. Vi beräknar antalet matriser vars determinant är lika med 0. I en sådan matris är kolonnerna linjärt beroende.

Antalet matriser vars första kolonn består av nollkolonnen är p^2.

Om första kolonnen är kolonnen $\bar{k} \neq \bar{0}$ så finns det precis p kolonner som tillsammans med $\bar{k}$ bildar en linjärt beroende mängd, nämligen kolonnerna $\lambda\bar{k}$ med $\lambda \in Z_p$. Alltså till varje kolonn $\bar{k} \neq \bar{0}$ finns det p stycken matriser med determinanten lika med 0 och med kolonnen $\bar{k}$ som första kolonn. Det finns $p^2 - 1$ sådana kolonner $\bar{k} \neq \bar{0}$ och antalet matriser med en determinant lika med noll blir alltså $p \cdot (p^2 - 1) = p^3 - p$.

Totalt finns alltså $p^3 - p + p^2$ matriser vars determinant är lika med 0. Så

SVAR: $p^4 - p^3 - p^2 + p$.

20. Undersök om mängden

$$Q(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in Q\},$$

där Q betecknar mängden av rationella tal, bildar en kropp.

Lösning: Precis på samma sätt som i uppgift 10 visas att $Q(\sqrt{2})$ är en ring. Den är kommutativ eftersom den är en delmängd till mängden av reella tal. Det som återstår är att visa att varje icke noll element är inverterbart.

Vi ger en explicit formel för inversen, som påminner om formeln för inverser till komplexa tal.

$$(a+b\sqrt{2})\frac{a-b\sqrt{2}}{a^2-2b^2} = \frac{(a+b\sqrt{2})(a-b\sqrt{2})}{a^2-2b^2} = 1,$$

och därmed är

$$(a+b\sqrt{2})^{-1} = \frac{a-b\sqrt{2}}{a^2-2b^2}.$$

Så det enda som återstår att kontrollera är att $a^2 \neq 2b^2$ för alla rationella tal a och b, eftersom vi inte kan dela med 0.

Men

$$a^2 = 2b^2 \quad \Rightarrow \quad \sqrt{2} = \frac{a}{b},$$

och då $\sqrt{2}$ är irrationellt men $\frac{a}{b}$ rationellt så kan det inte inträffa att $a^2 = 2b^2$. Eller kanske ännu mer generellt, polynomet $x^2 - 2$ är irreducibelt i ringen $Q[x]$ är det som avgör saken.