Matematiska Institutionen
KTH

Några övningar inför lappskrivning nummer 8, Diskret matematik för D2 och F, vt08.

1. 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.

2. 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

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

   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

   $$\begin{cases} A + C &= 0 \\ AC + 2 &= 1 \end{cases} \quad \text{resp} \quad \begin{cases} A + C &= 0 \\ AC - 2 &= 1 \end{cases}$$

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

3. 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:
$$\begin{aligned} x^5 + x^3 + x + 1 &= x^3(x^2 + 1) + x + 1 \\ x^2 + 1 &= (x + 1)(x + 1) + 0 \end{aligned},$$
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.

4. 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.

5. 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.

6. 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.

---

7. 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 $R = M_{3\times3}(Z_5)$ 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 $-A \in S$:

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

8. Betrakta ringen $R = M_{3\times3}(Z_3)$ 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: 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 $C = D^T$.

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

10. 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.

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

12. 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 6 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.