Matematiska Institutionen
KTH

Lösningar till inlämningsuppgift nummer 2 till kursen Diskret matematik för F3, F1spec, vt06.

1. Undersök om det finns en grupp G med 144 element som har delgrupper G_1, G_2 och G_3 med 12, 12 och 8 element och så att

$$G_1 \cap G_2 = \emptyset, \quad |G_1 \cap G_3| = 4, \quad |G_2 \cap G_3| = 2.$$

Lösning Grupperna G_1 och G_2 är delgrupper till G och innehåller samma identitetselement som G. Då kan inte deras snitt vara tomt. Alltså finns inga sådan grupper G_1 och G_2.

2. Rutorna på ett schackbräde med 64 rutor färgas antingen svarta eller vita. Hur många olika schackbräden kan man få om två schackbräden räknas som lika om man kan vrida det ena till det andra.

Lösning Gruppen G av tillåtna transformationer av schackbrädet består av fyra element: Om φ betecknar vridning 90 grader så är $G = \{\varphi, \varphi^2, \varphi^3, \varphi^4 = id\}$.

Vi använder Burnsides lemma

$$\text{antal olika schackbräden} = \frac{1}{|G|} \sum_{g \in G} |Fix_g|.$$

Med vanliga schackbeteckningar gäller att φ och φ^3kan beskrivas som en produkt av 16 stycken 4-cykler och φ^2 som en produkt av 32 stycken 2-cykler som i exemplet nedan:

$$\varphi = (a8\ h8\ h1\ a1) \cdots (d5\ e5\ e4\ d4)$$

För en färgläggning som är innehållen i Fix_φ gäller att den är konstant på alla 16 cyklerna som beskriver φ, dvs rutorna i cykeln $(a8\ h8\ h1\ a1)$ har alla samma färg.

Alltså måste $|Fix_\varphi| = 2^{16}$, $|Fix_{\varphi^2}| = 2^{32}$, $|Fix_{\varphi^3}| = 2^{16}$, $|Fix_{\varphi^4}| = 2^{64}$.

Svar $(2^{64} + 2^{32} + 2^{16} + 2^{16})/4$.

3. Låt F beteckna den ändliga kroppen med 16 element som erhålles med hjälp av kroppen Z_2 och det irreducibla polynomet $x^4 + x + 1$:

$$K = \{a_0 + a_1x + a_2x^2 + a_3x^3 \mid a_i \in Z_2, \ \ i = 0, 1, 2, 3\}$$

och där man räknar som om $x^4 = x + 1$.

(a) Lös i denna kropp ekvationen $z^2 - (x^3 + x)z + x^3 = 0$.

Lösning Prövning ger att elementet $x + 1$ är en rot. Produkten av ekvationens rötter är x^3. Alltså söker vi $x^3(x + 1)^{-1}$. Euklides algoritm ger

$$x^4 + x + 1 = (x^3 + x^2 + x)(x + 1) + 1.$$

Härur sluter vi att $(x + 1)^{-1} = x^3 + x^2 + x$. Den andra roten blir då lika med

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

Svar $x + 1$ och $x^3 + 1$.

(b) Bestäm en andragradsekvation som inte är lösbar i denna kropp.

Lösning Polynomet $x^4 + x + 1$ är primitivt och vi finner att

$$\begin{array}{rcl} x & = & x \\ x^2 & = & x^2 \\ x^3 & = & x^3 \\ x^4 & = & x+1 \\ x^5 & = & x^2+x \\ x^6 & = & x^3+x^2 \\ x^7 & = & x^3+x+1 \\ x^8 & = & x^2+1 \end{array} \qquad \begin{array}{rcl} x^9 & = & x^3+x \\ x^{10} & = & x^2+x+1 \\ x^{11} & = & x^3+x^2+x \\ x^{12} & = & x^3+x^2+x+1 \\ x^{13} & = & x^3+x^2+1 \\ x^{14} & = & x^3+1 \\ x^{15} & = & 1 \end{array}$$

Vi undersöker nu andragradsekvationer av typen

$$z(z+a) = 1 \quad \text{dvs} \quad z^{-1} = z + a.$$

Med $a = 1$ får vi t ex $(x^5)^{-1} = x^{10} = x^5 + 1$. Ekvationen $z(z+1) = 1$ har alltså roten $z = x^5$ och då är inte polynomet $z(z+1)+1$ irreducibelt. Nästa försök $a = x$ duger eftersom $x^t + a \neq x^{15-t}$ för alla värden på t.
Således

Svar Till exempel $z^2 + zx + 1$.

(c) Finns det någon kropp som innehåller K och i vilken din ekvation ovan är lösbar.

Lösning Låt F beteckna kroppen ovan med 16 element. Betraktar mängden av alla polynom

$$K = F[x] = \{a + bz \mid a, b \in F\}$$

och där man räknar som om $z^2 = xz + 1$. Mängden K utgör en kommutativ ring med etta och varje element har en invers, eftersom polynomet z^2+xz+1 är irreducibelt. Med hjälp av Euklides algoritm kan man till varje element $p(z)$ i K bestämma ett element $q(z)$ sådant att

$$p(z)q(z) + d(z)(z^2 + xz + 1) = 1,$$

och $p(z)^{-1} = q(z)$.