Matematiska Institutionen
KTH

Lösning till några övningar inför lappskrivning nummer 3 på moment B, Diskret matematik för D2 och F, vt09.

1. Betrakta den kropp med 8 element man får med hjälp av polynomet $p(x) = x^3+x+1$, dvs mängden
$$GF(8) = \{a_0 + a_1x + a_2x^2 \mid a_0, a_1, a_2 \in Z_2\},$$
och där man räknar som om $p(x) = 0$ dvs som om $x^3 = x + 1$.

   (a) Beräkna $(1 + x + x^2)(1 + x^2) + x + x^2$.

   Łösning: Med koefficienterna räknar vi modulo två och med potenser av x räknar vi som om x^3 kan ersättas med $x+1$. Vi får då emedan x^4 kan ersättas med $x \cdot x^3 = x(1 + x) = x + x^2$ att

   $$(1 + x + x^2)(1 + x^2) + x + x^2 = 1 + x^2 + x + x^3 + x^2 + x^4 + x + x^2 =$$
   $$= 1 + x^2 + x^3 + x^4 = 1 + x^2 + 1 + x + x(1 + x) = 0.$$

   (b) Bestäm inverserna till elementen $1 + x$, x och $x + x^2$.

   Łösning: Använder Euklides algoritm. Polynomdivision ger:

   $$x^3 + x + 1 \;=\; (x^2 + x)(x + 1) + 1$$

   varur (tänk på att $-1 = 1$ i ringen Z_2),

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

   Då vi skall räkna som om $x^3 + x + 1 = 0$ har vi alltså att $(x^2 + x)(x + 1) = 1$, så $(1 + x)^{-1} = x^2 + x$.
   Med Euklides algoritm får vi för x att

   $$x^3 + x + 1 \;=\; (x^2 + 1)x + +1.$$

   Med precis samma räkningar som ovan får vi att $x^{-1} = x^2 + 1$.
   För att bestämma inversen till $x + x^2$ utnyttjar vi att $x + x^2 = x(1 + x)$ så

   $$\begin{aligned}(x + x^2)^{-1} &= x^{-1}(1 + x)^{-1} = (x^2 + 1)(x^2 + x) = x^4 + x^3 + x^2 + x = \\ &= x(x^3 + x + 1) + x^3 = x \cdot 0 + x + 1.\end{aligned}$$

   (c) Lös ekvationen $(1 + x)z + x^2 = x$.

   Łösning: Vi får att

   $$z = (1 + x)^{-1}(x - x^2) = (1 + x)^{-1}(x + x^2) = (1 + x)^{-1}x(1 + x) = x.$$

(d) Bestäm tre olika generatorer till kroppens multiplikativa grupp.

Łösning: Den multiplikativa gruppen till kroppen F har $|F| = 8 - 1 = 7$ element. Varje element har en ordning som delar antalet element i gruppen. Endast elementet 1 har ordning 1, så alla andra element har ordning 7 och kan användas som generatorer till den multiplikativa gruppen. Tag vilka tre element som helst

Svar: T ex x, $1 + x$ och $1 + x^2$.

2. Kunstruera kroppar, eller motivera varför de inte går att konstruera, om kropparna skall ha

(a) 119 element.

Łösning: 119 är ingen primtalspotens eftersom $7 \cdot 17 = 119$. Antalet element i en ändlig kropp är alltid en potens av ett primtal. Så ingen kropp kan ha 119 element.

(b) 120 element.

Łösning: Samma motivering som ovan eftersom $120 = 2 \cdot 3 \cdot 20$ och alltså ingen primtalspotens.

(c) 121 element.

Łösning: Då $121 = 11^2$, en potens av primtalet 11, så finns en kropp med 121 element. För en konstruktion behövs ett irreducibelt polynom av grad 2 i polynomringen $Z_{11}[x]$. Söker ett sådant. Studerar för den skull mängden av kvadrater $\mathcal{Q}$ i ringen Z_{11}:

$$\mathcal{Q} = \{(\pm 1)^2 = 1, (\pm 2)^2 = 4, (\pm 3)^2 = 9, (\pm 4)^2 = 5, (\pm 5)^2 = 3\}.$$

Det finns alltså inget element x i Z_{11} sådant att $x^2 = 10 = -1$. Polynomet $p(x) = x^2 + 1$ saknar alltså nollställen och är således irreducibelt, eftersom det dessutom är av grad 2. Detta polynom definierar kroppen $GF(121)$ genom att man i mängden

$$GF(121) = \{a + bx \mid, a, b \in Z_{11}\},$$

räknar som om $x^2 = -1$.

3. En kropp $F = GF(27)$ med 27 element konstrueras med hjälp av det i polynomringen $Z_3[x]$ irreducibla polynomet $p(x) = x^3 + 2x + 2$.

(a) Bestäm x^4, x^5 och x^6.

Łösning: Vi använder att $x^3 = -2x - 2 = x + 1$, emedan $-2 = 1$ i Z_3, och får då

$$\begin{aligned} x^4 &= x \cdot x^3 = x(x+1) = x^2 + x \\ x^5 &= x \cdot x^4 = x(x^2 + x) = x^3 + x^2 = 1 + x + x^2 \\ x^6 &= x^3 \cdot x^3 = (1+x)^2 = 1 + 2x + x^2 = 1 - x + x^2. \end{aligned}$$

(b) Bestäm en generator α för kroppens multiplikativa grupp.

Lösning: Undersöker först om x genererar multiplikativa gruppen. Antalet element i denna grupp är 26, så x har då antingen ordning 2, 13 eller 26, vilka är delarna till 26. Elementen i F äro $a + bx + cx^2$ där a, b, c tillhör Z_3. Elementet x kan inte ha ordning 2 eftersom, eftersom 1 och x^2 faktiskt "par definition" är olika element i F:

$$1 = 1 + 0x + 0x^2 \neq 0 + 0x + x^2 = x^2.$$

Undersöker om x kan ha ordning 13.

$$\begin{aligned} x^{13} &= x^6 \cdot x^6 \cdot x = (1 - x + x^2)^2 x = \\ &= (1 + x^2 + x^4 - 2x + 2x^2 - 2x^3)x = (1 + x + x^3 + x^4)x = \\ &= (2 + x^2)x = 2x + x^3 = 1. \end{aligned}$$

Så x har ordning 13. Vad synd, men elementet 2 har ordning 2, (eftersom $2^2 = 1$) och då kan elementet $2x$ varken ha ordning 2 eller 13.

Svar: $\alpha = 2x$ till exempel.

(c) Bestäm k sådant att $\alpha^k = x^2 - 1$.

Lösning: Ser att $x^2 - 1 = x^2 + 2$. Observerar från räkningarna ovan att

$$1 = (2 + x^2)x = x^{13} = x^{12} \cdot x.$$

Så $x^{12} = 2 + x^2$, men $2^2 = 1$ och alltså $2^{12} = 1$, varur

$$\alpha^{12} = 2^{12}x^{12} = 1 \cdot (2 + x^2)$$

Svar $k = 12$.

(d) Har ekvationen $z^2 + xz + 1 = 0$ några rötter i kroppen? Bestäm i så fall dessa.

Lösning: En kvadratkomplettering ger, då $1 = -2$,

$$z^2 + xz + 1 = 0 \quad \Leftrightarrow \quad (z - x)^2 - x^2 + 1 = 0 \quad \Leftrightarrow \quad (z - x)^2 = x^2 - 1.$$

Vi vet från ovan att $x^2 - 1 = x^{12}$. Alltså har vi nu från ovan att

$$(z - x)^2 = x^{12} \quad \Rightarrow \quad (z - x) = \pm x^6 \quad \Rightarrow \quad (z - x) = \pm(1 - x + x^2),$$

så, då $-x = 2x$,

Svar: $z = x \pm (1 + 2x + x^2)$

4. Bestäm ett primitivt polynom $p(x)$ av grad två i ringen $Z_5[x]$. Detta polynom kan på sedvanligt sätt användas för att definiera en kropp F.

Łösning: Vi löser uppgift a) först.

(a) Hur många element kommer denna kropp att ha?

Łösning: 25 element eftersom den består av elementen i mängden

$$GF(25) = \{a + bx \mid a, b \in Z_5\}.$$

där man räknar som om $p(x) = 0$ för något irreducibelt polynom $p(x)$ av grad 2.

Polynomet $p(x)$ är primitivt om x kommer att generera den multiplikativa gruppen som i detta fall består av 24 element (alla element utom nollan). Vi använder metoden med "trial and error".

Provar först med poynomet $p(x) = x^2 - x - 1$. Vi finner att $p(1) = -1$, $p(2) = 1$, $p(3) = 0$ så polynomet hat nollställen och är då inte ens irreducibelt.

Nytt försök med $p(x) = x^2 + x + 2$, $p(1) = 4$, $p(2) = 3$, $p(3) = 4$, $p(4) = 2$ så inga nollställen och i varje fall ett irreducibelt polynom (eftersom polynomet är av grad 2 och saknar nollställen). Testar om x genererar multiplikativa gruppen, dvs om x har ordning 24.

Vi finner

$$\begin{aligned} x^2 &= -x - 2 \\ x^3 &= -x^2 - 2x = x + 2 - 2x = -x + 2 \\ x^6 &= (-x + 2)^2 = x^2 - 4x + 4 = -x - 2 - 4x + 4 = 2 \\ x^{12} &= 2^2 = -1 \neq 1 \end{aligned}$$

och då kan ej heller $x^4 = 1$ ty då vore $x^{12} = (x^4)^3 = 1^3 = 1$. Ordingen av elementet x delar talet 24, men är varken lika med 1, 2, 3, 4, 6 eller 12. Enda möjligheten är att x har ordning 24 och genererar kroppens multiplikativa grupp.

Svar: T ex polynomet $p(x) = x^2 + x + 2$.

(b) Bestäm tre olika generatorer för kroppens multiplikativa grupp.

Łösning: Vet att kroppens multipliktiva grupp är cyklisk, och vet om cykliska grupper att om x är en genareator så kommer även x^a att vara en generator för alla a sådana att $sgd(a, n) = 1$. där n är antalet element i gruppen, i detta fall $n = 24$.

Svar: Till exempel x^5, x^7 och x^{11}.

(c) Bestäm samtliga lösningar i F till ekvationen $z^3 = 1$.

Lösning: Eftersom gruppen är cyklisk och talet 3 delar antalet element i gruppen finns precis tre olika lösningar. Med x som generator är dessa

Svar: x^8, x^{16} och $x^{24} = 1$.

(d) Bestäm samtliga lösningar i F till ekvationen $z^5 = 1$.

Łösning: Eftersom x genererar multiplikativa gruppen kan varje element z i kroppen uttryckas som $z = x^a$ för något heltal a. Antag att $(x^a)^5 = 1$ för något tal a. Då skulle

$$x^{5a} = 1,$$

och enligt känd sats, gruppens ordning dela talet $5a$. Men

$$24 \mid 5a \qquad \Rightarrow \qquad 24 \mid a,$$

och då skulle

$$x^a = x^{24t} = (x^{24})^t = 1^t = 1.$$

Svar: Endast en lösning till ekvationen, nämligen $z = 1$.

5. Kan en kropp med 64 element ha en delkropp med

(a) 2 element?

Łösning: Ja alla kroppar innehåller sin s k primkropp, mer precist: en kropp med p^k element, där p är ett primtal, innehåller alltid kroppen Z_p, kroppens primkropp, som delkropp. Vi har $32 = 2^5$ så primkroppen är Z_2.

(b) 32 element?

Łösning: Nej, ty multiplikativa gruppen H till kroppen med 32 element vore då en delgrupp till multiplikativa gruppen G till kroppen med 64 element. Då skulle, enligt Lagranges sats, $|H|$ dela $|G|$, dvs 31 del 63, men så är ju inte fallet.

6. Konstruera en kropp med 64 element som har en delkroppp med 8 element. Kommer varje kropp med 64 element att ha en delkropp med 8 element?

Łösning: Låt F vara den kropp med 8 element som erhålls med hjälp av polynomet $p(x) = x^2 + x + 1$ som i uppgift 1. Söker nu ett irreducibelt andragradspolynom $q(z)$ i polynomringen $F[z]$. Mängden

$$K = \{\alpha + \beta z \mid \alpha, \beta \in F\},$$

kommer då att bilda en kropp om vi räknar som om $q(z)$ vore lika med noll.

Söker $q(z)$. Listar upp samtliga element i F:

$$\begin{aligned} x &= x, \\ x^2 &= x^2, \\ x^3 &= x + 1, \\ x^4 &= x^2 + x, \\ x^5 &= x^3 + x^2 = x^2 + x + 1 \\ x^6 &= x^2 + 1, \\ x^7 &= 1. \end{aligned}$$

Vi ser, okular besiktning, att det aldrig inträffar att $z^2 - z = 1$, för något element z i kroppen F. Så $q(z) = z^2 + z + 1$ är irreducibelt i polynomringen $F[z]$ och kroppen är konstruerad enligt receptet ovan.

Det finns bara en kropp med 64 element, så när som på isomorfi, så alla kroppar, den enda dvs, med 64 element kommer att ha en delkropp med 8 element.