Matematiska Institutionen
KTH

Lösningar till tentamensskrivning i Diskret matematik, moment B, för F och D, SF1630B resp SF1631B, den 20 augusti 2008.

1. Vi finner att $n = 51 = 3 \cdot 17$ så $m = 2 \cdot 16 = 32$. Eftersom e och d skall uppfylla $e \cdot d \equiv 1 \pmod{m}$ kan vi t ex välja $e = 11$ och d lika med 3. Då blir $D(2) = 2^3 = 8$.

   SVAR: Med $e = 11$ så får vi $D(2) = 8$.

2. Vi finner att
$$2^2 + 2 + 1 = 0$$
i ringen Z_7. Polynomet har alltså ett nollställe i denna ring och kan då inte vara irreducibelt.

   Svar Polynomet är inte irreducibelt.

3. (a) Vi skall leta rätt på ett element med (multiplikativ) ordning 12. Vi vet att ordningen av ett element i gruppen alltid delar talet 12, så möjliga ordningar är 1, 2, 3, 4, 6 eller 12. Vi börjar med att testa om elementet 2 har ordning 12:
$$2^2 = 4 \neq 1, \quad 2^3 = 8 \neq 1, \quad 2^4 = 3 \neq 1, \quad 2^6 = 2^2 \cdot 2^4 = 4 \cdot 3 = 12 \neq 1.$$
   Enda möjligheten är att elementet 2 har ordning 12. Detta element är då en generator för gruppen.

   (b) Elementen i mängden
$$H = \{2^2, 2^4, 2^6, 2^8, 2^{10}, 2^{12}\} = \{4, 3, 12, 9, 10, 1\},$$
   bildar en grupp med sex element.

4. Strukturen är inte en grupp, ty ur tabellen framgår att e är identiteselementet (eftersom $eg = g$ för varje element $g \in G$) och i varje grupp gäller för alla element $g \in G$ att $g \cdot g^{-1} = e = g^{-1} \cdot g$. Men $d \cdot a = e$ och $a \cdot d = b \neq e$.

5. Gruppen $(Z_{20}, +)$ har precis en delgrupp med fem element nämligen mängden
$$H = \{0, 4, 8, 12, 16\}.$$
   Sidoklassen
$$3 + H = \{3, 7, 11, 15, 19\},$$
   är den sökta sidoklassen.

6. Den givna kroppen har nio element och dess multiplikativa grupp, dvs de element som inte är noll består av åtta element. Om ett element z satisfierar att $z^6 = 1$ så vet vi från den allmänna teorin om grupper att ordningen av elementet måste dela 6. Vidare då elementet z ligger i en grupp av ordning åtta så måste z ha en ordning som delar 8. Den största gemensamma delaren till 8 och 6 är 2. Så det sökta elementet har antingen ordning 1, dvs är elementet 1, eller har ordning 2. Det finns bara ett element med ordning 2, nämligen elementet -1 som ju är lika med 2.

   SVAR: 2

7. (a) Då C är linjär så kommer varje linjärkombination

$$\lambda_1 c_1 + \lambda_2 c_2 + \lambda_3 c_3$$

att tillhöra C. T ex kommer ordet

$$c_1 + c_2 + c_3 = 000000110,$$

att tillhöra C. Men eftersom nollordet tillhör C och ordet ovan har avstånd två till nollordet så skulle inte koden vara 1-felsrättande om detta ord tillhörde C.

(b) Vi konstruerar en kontrollmatris H med 4 rader och 9 kolonner. Den 1-felsrättande kod C som denna matris då definierar kommer att ha $2^{9-4} = 32$ stycken ord. Matrisen H kommer att bestå av nio olika kolonner. Ordet c_1 finns med i C precis då summan av de fyra första kolonnerna blir noll, och en motsvarande reltion mellan andra kolonner skall gälla för att ordet c_2 skall finnas med i C. Lite trial and error ger följande matris (observera att matrisens kolonner också måste vara olika):

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

V hittade en kontrollmatris som ger en 1-felsrättande kod med 32 ord och som innehåller orden c_1 och c_2. Så svaret är JA.

8. Betrakta en platta med fyra hörn numrerade i tex högerled 1,2,3,4. Vridningarna av plattan ger en grupp G med åtta element:

$$G = \{(1), \varphi = (1\ 2\ 3\ 4), \varphi^2, \varphi^3, (1\ 2)(3\ 4), (1\ 3), (2\ 4), (1\ 4)(2\ 3)\},$$

som ju uppenbarligen är en delgrupp till $\mathcal{S}_4$.

9. Låt G beteckna den direkta produkten $G_1 \times G_2$.

(a) Enligt en känd sats är alla delgrupper till en cyklisk grupp cykliska. Gruppen G_1 är isomorf med delgruppen $H_1 = G_1 \times \{e\}$ till G, där e betecknar identitetselementet i G_2. Eftersom H_1 är cyklisk så måste även G_1 vara cyklisk. På samma sätt visas att G_2 är cyklisk.

Vår slutsats blir att grupperna G_1 och G_2 båda måste vara cykliska om G är cyklisk.

(b) Enligt en sats i boken är en grupp med n element cyklisk om och endast om den har precis en delgrupp med d element för varje delare d till n. Låt n_1 och n_2 beteckna antalet element i G_1 respektive G_2. Om d delar både n_1 och n_2 så har G_1 och G_2 delgrupper H_1 och H_2 båda med d stycken element. Grupperna $H_1 \times \{e\}$och $\{0\} \times H_2$ är då två olika delgrupper till G, båda med d element och då kan inte G vara cyklisk.

Om n_1 och n_2 är relativt prima och med generatorer g_1 respektively g_2 så kommer elementet (g_1, g_2) att ha ordning n och vara en generator till G som alltså då är cyklisk.

Alltså är G cyklisk precis då talen n_1 och n_2 är relativt prima.

10. Vi löser båda deluppgifterna samtidigt. Låt F beteckna den kropp som definieras med hjälp av polynomet $x^3 + x + 1$ och låt K beteckna den andra kroppen i fråga och låt φ beteckna en isomorfi från F till K.

Eftersom $\varphi(a \cdot b) = \varphi(a)\varphi(b)$ så får vi

$$\varphi(1) = \varphi(1 \cdot 1) = \varphi(1)\varphi(1)$$

och alltså är $\varphi(1) = 1$.

I kroppen F gäller att $x^3 + x = 1$. Eftersom $\varphi(a + b) = \varphi(a) + \varphi(b)$ får vi att

$$1 = \varphi(1) = \varphi(x^3 + x) = \varphi(x^3) + \varphi(x) = \varphi(x)^3 + \varphi(x).$$

Alltså måste $\varphi(x) = z \in K$ där z sådant att $z^3 + z = 1$. Vi tar nu reda på precis vilka element i K som uppfyller detta. Vi gör först en tabell över elementen i K:

$x^3 = x^2 + 1$,
$x^4 = x \cdot x^3 = x(x^2 + 1) = x^3 + x = x^2 + x + 1$,
$x^5 = x(x^2 + x + 1) = x^3 + x^2 + x = x + 1$,
$x^6 = x(x + 1) = x^2 + x$,
$x^7 = 1$

I K gäller att $x^3 + x^2 = 1$ så vi får med hjälp av tabellen ovan

$$\begin{array}{llrcl}
z = 1: & z^3 + z = & 1^3 + 1 & = & 0 \neq 1, \\
z = x: & z^3 + z = & x^3 + x & = & x^2 + 1 + x \neq 1, \\
z = x^2: & z^3 + z = & x^6 + x^2 & = & x^2 + x + x^2 = x \neq 1, \\
z = x^3: & z^3 + z = & x^9 + x^3 & = & x^2 + x^2 + 1 = 1, \\
z = x^4: & z^3 + z = & x^{12} + x^4 & = & x^5 + x^4 = x + 1 + x^2 + x + 1 = x^2 \neq 1, \\
z = x^5: & z^3 + z = & x^{15} + x^5 & = & x + x^5 = x + x + 1 = 1, \\
z = x^6: & z^3 + z = & x^{18} + x^6 & = & x^4 + x^6 = x^2 + x + 1 + x^2 + x = 1.
\end{array}$$

Det finns alltså högst tre olika isomorfier φ_i, $i = 1, 2, 3$, från F till K och som, om de vore isomorfier, skulle definieras av $\varphi_1(x) = x^3 \in K$, $\varphi_2(x) = x^5 \in K$ samt $\varphi_3(x) = x^6 \in K$. Vi kommer att visa att φ_1 är en isomorfi. Att de andra är isomorfier inses på samma sätt.

Definiera $\varphi_1(x^n) = z^n$ där $z = x^3 \in K$. Då gäller att, eftersom x genererar F och $x^3 \in K$ genererar K (eftersom x^3 har ordning 7 i K:s multiplikativa grupp), φ_1 är en bijektion. Dessutom kommer

$$\varphi_1(x^n \cdot x^m) = \varphi_1(x^{n+m}) = z^{n+m} = z^n \cdot z^m = \varphi_1(x^n) \cdot \varphi_1(x^m),$$

och alltså gäller att $\varphi_1(a \cdot b) = \varphi_1(a) \cdot \varphi_1(b)$ för alla $a, b \in F$. Vi verifierar nu att $\varphi_1(a + b) = \varphi_1(a) + \varphi_1(b)$ genom att först visa detta när $a = 1$ och $b = x^n$, för $n = 1, 2, 3, \ldots, 7$.

$$\varphi_1(1 + x) = \varphi_1(x^3) = z^9 = x^2 (\in K) \quad \text{och} \quad \varphi_1(1) + \varphi_1(x) = 1 + z = 1 + x^3 = x^2.$$

etc. När detta är gjort får vi

$$\varphi_1(x^n + x^m) = \varphi_1(x^n(1 + x^{m-n})) = \varphi_1(x^n)(\varphi_1(1) + \varphi_1(x^{m-n})) = \varphi_1(x^n) + \varphi(x^{m-n+n}),$$

och isomorfin hos φ_1 är verifierad. (Det finns mer abstrakta, och mindre räknekrävande sätt, att också visa isomorfin på. T ex kan man låta L_1 beteckna mängden

$$L_1 = \{a_0 + a_1 z + a_2 z^2 \mid a_0, a_1, a_2 \in Z_2\},$$

där man räknar som om $z^3 + z + 1 = 0$. Mängden L_1 blir då en kropp med nio element som uppenbarligen är isomorf med F, via den triviala isomorfin $\psi(x) = z$. Med $z = x^3$, där $x \in K$, tillhör alla element i L_1 kroppen K. Vidare är räkneregeln $z^3 + z + 1$ härledd under additionen och mutiplikationen i K. Således är

$$L_1 = \{a_0 + a_1 x^3 + a_2 x^6 \mid a_0, a_1, a_2 \in Z_2\} = K$$

och man räknar som om $x^3 + x^2 + 1 = 0$, dvs L_1 och K är samma kropp.)