Matematiska Institutionen
KTH

Lösning till några övningar inför lappskrivning nummer 4, Diskret matematik för D2 och F, vt10.

1. Det går att fylla i nedanstående tabell så att den blir multiplikationstabellen till en grupp. Gör detta.

$\circ$	a	b	c	d	f	g
a	a	b				
b				f	d	c
c		f	a		b	
d			f		c	b
f			d			a
g		d			a	f

Lösning:

$\circ$	a	b	c	d	f	g
a	a	b	c	d	f	g
b	b	a	g	f	d	c
c	c	f	a	g	b	d
d	d	g	f	a	c	b
f	f	c	d	b	g	a
g	g	d	b	c	a	f

(a) Ange gruppens identitetselement.

Lösning: a, ty det gäller att $a \circ b = b$ varur vi erhåller att

$$a \circ b \circ b^{-1} = b \circ b^{-1} = id,$$

där id just nu betecknar gruppens identitetselement.

(b) Är gruppen abelsk.

Lösning: Nej ty multiplikationstabellen är inte symmetrisk runt den sk huvuddiagonalen. Till exempel gäller att $b \circ c = g$ men $c \circ b = f \neq g$.

(c) Bestäm inverser till alla element.

Lösning: $a^{-1} = a$, $b^{-1} = b$, $c^{-1} = c$, $d^{-1} = d$, $f^{-1} = g$ och $g^{-1} = f$.

(d) Bestäm ordningen av alla element.

Lösning: $\sigma(a) = 1$, $\sigma(b) = 2$, $\sigma(c) = 2$, $\sigma(d) = 2$, $\sigma(f) = 3$, $\sigma(g) = 3$, ty t ex $f \circ f = g$ och $f \circ f \circ f = a$.

(e) Beräkna $b \circ c \circ d \circ f \circ g$.

Lösning: $b \circ c \circ d \circ f \circ g = b \circ c \circ d \circ a = b \circ c \circ d = b \circ g = c$

(f) Bestäm delgrupper med två respektive tre element.

Lösning: Tar element av ordning två respektive tre och låter dessa generera cykliska grupper. De möjliga delgrupperna blir då

$$
\begin{aligned}
&< b >= \{b, b \circ b = a\}, \\
&< c >= \{c, c \circ c = a\}, \\
&< d >= \{d, d \circ d = a\}, \\
&< f >= \{f, f \circ f = g, f \circ f \circ f = a\}
\end{aligned}
$$

.

(g) Bestäm vänster och höger sidoklasser till de delgrupper du fann ovan.

Lösning: $\{a, b\}$ har höger sidoklasserna $\{a, b\}$, $\{a \circ c, b \circ c\} = \{c, g\}$, $\{a \circ d, b \circ d\} = \{d, f\}$ och vänster sidoklasser $\{a, b\}$, $\{c \circ a, c \circ b\} = \{c, f\}$, $\{d \circ a, d \circ b\} = \{d, g\}$. och så vidare.

2. Visa att $G = (Z_{13} \setminus \{0\}, \cdot)$ är en grupp och bestäm ordningen av samtliga element i G. Är G en cyklisk grupp?

Lösning: Associativa lagen gäller allmänt vid multiplikation i Z_{13} och därför också i G. Identitetselement finns eftersom elementet 1 tillhör G. Alla element i G är inverterbara eftersom 13 är ett primtal och eftersom det gäller allmänt i en ring Z_n att a är inverterbart precis då $sgd(a, n) = 1$. G består alltså av de inverterbara elementen i Z_{13}. Produkten av inverterbara element är ett inverterbart element, eftersom om a och b har inverseerna a^{-1} resp b^{-1} så är

$$ab \circ b^{-1}a^{-1} = a \circ bb^{-1} \circ a^{-1} = a \circ e \circ a^{-1} = aa^{-1} = e,$$

dvs $(ab)^{-1} = b^{-1}a^{-1}$. Alltså är G också sluten med avseende på multiplikation. Vi har nu visat att G är en grupp.

Nu till ordningen av elementen. Allmänt gäller ju att ordningen av ett element i en grupp G delar antalet elenment i G.

Vi börjar med elementet 2. Vi vet att $\sigma(2) \mid 12$ eftersom G har 12 element. Vi finner att $2^2 = 4 \neq 1$, $2^3 = 8 \neq 1$, $2^4 = 3 \neq 1$, $2^6 = 12 \neq 1$. Alltså kan vi dra den slutsatsen att $\sigma(2) = 12$ och att G genereras av elementet 2, dvs

$$G =< 2 >= \{2, 2^2, 2^3, \ldots, 2^{12} = 1\}.$$

Gruppen G är alltså cyklisk.

Vi kan nu gå igenom samtliga övriga 11 element på samma sätt för att bestämma dessa elements ordningar. Men vi kan också utnyttja att elementet 2 genererar hela gruppen, dvs om vi räknar modulo 13 så får vi

$$G = \{1, 2, 2^2 = 4, 2^3 = 8, 2^4 = 3, 2^5 = 6, 2^6 = 12, 2^7 = 11, 2^8 = 9, 2^9 = 5, 2^{10} = 10, 2^{11} = 7\}.$$

Om vi nu utnyttjar att

$$2^{12} = 1$$

så får vi att $3 = 2^4$ har ordning 3, eftersom

$$3^2 = (2^4)^2 = 2^8 = 9 \neq 1, \qquad \text{men} \qquad 3^3 = (2^4)^3 = 2^{12} = 1.$$

På samma sätt får vi att $4 = 2^2$ har ordning 6, $5 = 2^9$ har ordning 4, $6 = 2^5$ har ordning 12, $7 = 2^{11}$ har ordning 12, $8 = 2^3$ har ordning 4, $9 = 2^8$ har ordning 3, $10 = 2^{10}$ har ordning 6, $11 = 2^7$ har ordning 12, och $12 = 2^6$ har ordning 2.

3. Gruppen H är en delgrupp till en grupp G. Antag H består av 13 element och att det finns 7 sidoklasser till H i G.

(a) Hur många element består då G av.

Lösning: Sidoklasserna delar in gruppen i disjunkta delmängder som är lika stor som delgruppen. Alltså är antalet element i G lika med

$$|G| = 13 \cdot 7 = 91.$$

(b) Ge exempel på en grupp G med en delgrupp H som uppfyller dessa förutsättningar.

Lösning: Tag $(Z_{91}, +)$ och låt $H = \{0, 7, 14, 21, 28, 35, 42, 49, 56, 63, 70, 77, 84\}$.

4. Visa att $(Z_{10}, +)$ är isomorf med $(Z_2, +) \times (Z_5, +)$.

Lösning: Båda grupperna är cykliska med generatorer 1 respektive $(1, 1)$. Vi definierar en funktion φ från $(Z_{10}, +)$ till $(Z_2, +) \times (Z_5, +)$ genom

$$\varphi(k) = (k(\text{mod } 2), k(\text{mod } 5)).$$

Då gäller, enligt Kinesiska restsatsen, att
(i) $\varphi(k)$ är en bijektion
samt att
(ii) $\varphi(k_1 + k_2) = \varphi(k_1) + \varphi(k_2)$ för alla element $k_1 \in (Z_2, +)$ och $k_2 \in (Z_5, +)$,
eftersom

$$\varphi(k_1 + k_2) = ((k_1 + k_2)(\text{mod } 2), (k_1 + k_2)(\text{mod } 5)) =,$$
$$(k_1(\text{mod } 2), k_1(\text{mod } 5)) + (k_2(\text{mod } 2), k_2(\text{mod } 5)) = \varphi(k_1) + \varphi(k_2).$$

Alltså är φ en isomorfi och grupperna är isomorfa.

---

5. Undersök om det går att fylla i nedanstående tabell så att den blir multiplikationstabellen till en grupp.

$\circ$	a	b	c	d	f	g	h
a		b					
b		a					
c							
d							
f							
g							
h							

Lösning: Eftersom $a \circ b = b$ så måste a vara gruppens identitetselement. Det gäller också då att $b \circ b = a$ så ordningen av b måste vara två. Men eftersom gruppen har sju element så delar inte ordningen av elementet b antalet element i gruppen vilket strider mot en av de generella satserna för grupper. Alltså finns ingen grupp tabell sådan att $a \circ b = b$ och $b \circ b = a$.

6. En grupp G har delgrupper H och K med vardera 15 respektive 21 element. Vilka möjligheter finns det för antalet element i G.

Lösning: Enligt Lagranges sats måste både antalet element i H och antalet element i K dela antalet element G, dvs $15 \mid |G|$ och $21 \mid |G|$ vilket leder till att 105 måste dela antalet element i gruppen G.

Betrakta nu gruppen $G_1 = (Z_{105}, +)$. Den har delgrupperna

$$H = \{0, 7, 14, 21, \ldots, 98\} \qquad \text{och} \qquad K = \{0, 5, 10, 15, 20, \ldots, 100\}$$

med respektive 15 och 21 element. Det finns alltså en grupp med 105 element som uppfyller de givna förutsättningarna.

Betrakta nu G_2 vara vilken annan grupp som helst med identiteslementet e och låt G vara gruppen

$$G = G_1 \times G_2 = \{(g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2\},$$

och med komponentvis gruppoperationer i G_1 resp G_2 som gruppoperation i G. Då gäller att antalet element i G är $|G_1| \cdot |G_2|$ dvs

$$|G| = 105 \cdot |G_2|$$

och att G har följande delgrupper med respektive 15 och 21 element.

$$H \times \{e\} \qquad \text{och} \qquad K \times \{e\}.$$

SVAR: Om och endast om $|G| = 105n$, $n = 1, 2, 3, 4, \ldots$, finns en grupp G med delgrupper om 15 respektive 21 element.

7. Bestäm en abelsk grupp med 12 element och som är sådan att inget element har ordning 4.

Lösning: Betrakta den abelska gruppen

$$G = Z_2 \times Z_2 \times Z_3 = \{(a, b, c) \mid a, b \in Z_2, c \in Z_3\},$$

med komponentvis addition i respektive ringar som gruppoperation.

Om $c \neq 0$ så blir för varje val av $a, b \in Z_2$

$$(a, b, c) + (a, b, c) + (a, b, c) + (a, b, c) = (0, 0, c) \neq (0, 0, 0),$$

och sådana element (a, b, c) kan således inte ha ordning fyra.

För övriga element i G, dvs de med $c = 0$ gäller att

$$(a, b, 0) + (a, b, 0) = (0, 0, 0),$$

eftersom a och b är element i ringen Z_2. Elementen $(a, b, 0)$ har alltså ordning 2.

I gruppen G fanns alltså inga element av ordning 4 att finna.

8. Bestäm samtliga grupper med 149 element.

Lösning: Inget av primtalen 2, 3, 5, 7 eller 11 är delare till talet 149 och $13^2 > 149$. Detta medför att talet 149 är ett primtal. Varje element i en grupp G med 149 element har en ordning som delar 149. Så om ordningen av element $g \in G$ inte är lika med 1 så måste elementets ordning vara 149. Elementet g genererar då hela gruppen, dvs $G =< g >= \{g, g^2, g^3, \ldots, g^{149} = e\}$ och gruppen är cyklisk. Vår slutsats är alltså att alla grupper med 149 element är cykliska och kommer då att vara isomorfa med gruppen G ovan, eller också om man så vill isomorfa med den cykliska gruppen $(Z_{149}, +)$.

SVAR: Varje grupp med 149 element är cyklisk