EXEMPELSAMLING TILL

PÅBYGGNADSKURS

ALGEBRA I

Copyright: Matematiska institutionen
Stockholms universitet
1974

Eftertryck förbjudes

INNEHÅLL

		sid
BRUKSANVISNING		1
INTRODUKTION OCH REPETITION (I)		
Uppgifter		3
Svar		7
Ledningar		9
Lösningar		10
GRUPPER (G)		
Uppgifter	GA	13
	GB	21
	GC	27
Svar	GA	31
	GB	34
	GC	35
Ledningar	GA	36
	GB	39
	GC	43
Lösningar	GA	45
	GB	51
	GC	58
RINGAR (R)		
Uppgifter	RA	62
	RB	72
	RC	81
Svar	RA	85
	RB	90
	RC	94
Ledningar	RA	96
	RB	99
	RC	102
Lösningar	RA	105
	RB	111
	RC	119
KROPPAR (K)		
Uppgifter	KA	123
	KB	126
	KC	129
Svar	KA	131
	KB	132
	KC	133
Ledningar	KA	134
	KB	135
	KC	136
Lösningar	KA	137
	KB	141
	KC	146

Följande standardbeteckningar har använts:

$\mathbb{Z}$ = heltalen

$\mathbb{Q}$ = de rationella talen

$\mathbb{R}$ = de reella talen

$\mathbb{C}$ = de komplexa talen

$\mathbb{Z}_+, \mathbb{Q}_+, \mathbb{R}_+$ betecknar mängden av positiva tal i resp. talmängd

$\mathbb{Z}_n$ = restklasserna av $\mathbb{Z}$ modulo n

$\overline{a}$ = den restklass modulo n som innehåller a

(a,b) = största gemensamma divisorn till a och b

$a \mid b$ betyder att a delar b.

Introduktion och repetition

Funktioner, relationer, heltalen, restklasser modulo n.

I 1 Avgör för var och en av följande avbildningar från Z till Z om den är på resp. 1-1:

a) $x \to 3x$ b) $x \to x + 2$ c) $x \to x^2$.

I 2 Låt S och T vara delmängder av R, sådana att $x \to x^2$ är en funktion från S till T. I vilka av följande fall är funktionen på resp. 1-1?

a) $S = T = \mathbb{R}$

b) $S = \mathbb{R}$ och T = de icke-negativa reella talen

c) S = de icke-negativa reella talen och $T = \mathbb{R}$

d) S = T = de icke-negativa reella talen.

I 3 Låt f och g vara funktioner sådana att $f \circ g$ är definierad.

a) Om $f \circ g$ är på, måste då någon av f och g vara på? I så fall vilken? Måste båda vara på? Bevisa eller ge motexempel.

b) Samma frågor som i a) med på utbytt mot 1-1.

I 4 Låt S vara en ändlig mängd och $f: S \to S$ en funktion. Visa

a) om f är på, så är f 1-1 b) om f är 1-1, så är f på.

c) Visa också med exempel att påståendena i a) och b) är falska för en funktion från en icke-ändlig mängd till sig själv.

I 5 Bestäm vilka av de nedanstående relationerna som är ekvivalensrelationer på mängden S. Ange i förekommande fall ekvivalensklasserna.

a) $S = \mathbb{Z}$ och $a \sim b$ om $|a - b| < 3$

b) $S = \mathbb{R}$ och $a \sim b$ om det finns $q \in \mathbb{Q}_+$ så att $a = b + \ln q$

c) $S = \mathbb{C} \setminus \{0\}$ och $a \sim b$ om a/b är ett positivt reellt tal

d) $S = \mathbb{R}$ och $a \sim b$ om $ab > 0$

e) $S = \mathbb{Z}_+$ och $a \sim b$ om a/b är ett udda heltal

f) S = {deriverbara funktioner $\mathbb{R} \to \mathbb{R}$} och $f \sim g$ om $f' = g'$

g) S = {inverterbara 2 x 2-matriser} och $A \sim B$ om $\det(AB^{-1}) = 1$

h) S = {icke-tomma delmängder av en mängd M} och $E \sim F$ om $E \cap F \neq \emptyset$

I 6 På $\mathbb{Z}_+$ ges en relation: $a \sim b$ om $ab = n^2$ för något heltal n. Visa att detta är en ekvivalensrelation på $\mathbb{Z}_+$. Vilka är elementen i E(1) = den ekvivalensklass som bestäms av 1? I E(2)?

I 7 a) Bestäm (360,539) med Euklides' algoritm.

b) Euklides' algoritm ger den sista icke-försvinnande resten r_n = (360,539). Uttryck med hjälp av den sista divisionen r_n i r_{n-1} och r_{n-2}. I näst sista steget i Euklides' algoritm kan r_{n-1} uttryckas i r_{n-2} och r_{n-3}. Använd detta för att uttrycka r_n i r_{n-2} och r_{n-3}. Fortsätt på detta sätt baklänges i Euklides' algoritm till dess r_n är uttryckt i 360 och 539.

c) Bestäm heltal s och t så att 360s + 539t = (360,539).

I 8 Bestäm (819,287) och skriv den på formen 819s + 287t för några heltal s och t.

I 9 Finns heltal s och t så att

a) 7s + 81t = 1 b) 7s + 91t = 1 ?

I 10 a,b och c är heltal.

a) Visa att om ax + by = 1 har heltalslösning, så är (a,b) = 1.

b) Visa att om (a,b) = 1, så har ax + by = 1 heltalslösning.

c) Försök bestämma nödvändigt och tillräckligt villkor för att ekvationen ax + by = c skall ha heltalslösning.

I 11 Vilken är den minsta icke-negativa resten vid division med 7 av:

a) 87 + 51 b) 721 + 314 c) 87.51 d) 721.314.

I 12 Visa att $6 \mid (n^3 - n)$ för alla heltal n.

I 13 Visa att $14 \mid (21^n + 7^n)$ för alla $n \in \mathbb{Z}_+$.

I 14 Avgör vilka av följande påståenden som är sanna och vilka som är falska. Bevisa de sanna och ge motexempel till de falska.

a) $b \mid (a^2 + 1) \implies b \mid (a^4 + 1)$

b) $c \mid a$ och $d \mid b \implies (cd) \mid (ab)$

c) p primtal, $p \mid a$ och $p \mid (a^2 + b^2) \implies p \mid b$.

I 15 Gör additions- och multiplikationstabeller för a) $\mathbb{Z}_5$, b) $\mathbb{Z}_6$ (dvs. fyll i summor och produkter i tabeller av formen

	$\bar{0}$	$\bar{1}$	$\bar{2}$	. . .	$\bar{n}$
$\bar{0}$					
$\bar{1}$					
.					
$\bar{n}$					

$(n = 4,5)$).

I 16 Gäller $\bar{a}.\bar{b} = \bar{0} \implies (\bar{a} = \bar{0}$ eller $\bar{b} = \bar{0})$ i a) $\mathbb{Z}_5$, b) $\mathbb{Z}_6$?

I 17 Visa att om $\bar{a} \in \mathbb{Z}_5$ och $\bar{a} \neq \bar{0}$ så finns $\bar{b} \in \mathbb{Z}_5$ så att $\bar{a}.\bar{b} = \bar{1}$. Gäller motsvarande påstående i $\mathbb{Z}_6$?

I 18 Avgör, t.ex. genom prövning, om ekvationerna (i) $\bar{2}.x = \bar{1}$, (ii) $\bar{3}.x = \bar{1}$, (iii) $\bar{5}.x = \bar{1}$ har lösning i

a) $\mathbb{Z}_{10}$, b) $\mathbb{Z}_{11}$, c) $\mathbb{Z}_{12}$.

I 19 a) För vilka element $\bar{a} \in \mathbb{Z}_8$ finns $\bar{b} \in \mathbb{Z}_8$ så att $\bar{a}.\bar{b} = \bar{1}$?

b) Samma uppgift som i a) för $\mathbb{Z}_9$.

c) Samma uppgift som i a) för $\mathbb{Z}_{10}$.

I 20 a) Ange ett nödvändigt och tillräckligt villkor på a och n för att ekvationen $\bar{a}.x = \bar{1}$ skall ha lösning i $\mathbb{Z}_n$.

b) Bevisa det påstående Du formulerat i a).

I 21 Eulers ϕ-funktion på $\mathbb{Z}$ definieras på följande sätt:

$\phi(1) = 1$ och för $n > 1$ är $\phi(n)$ = antalet positiva heltal a, sådana att $a < n$ och $(a,n) = 1$.

a) Bestäm $\phi(n)$ för $n = 3,4,\ldots,20$.

b) Vad är $\phi(p)$ för p primtal?

c) Visa att $\phi(p^k) = p^{k-1}(p - 1)$ för p primtal, k positivt heltal.

d)* Visa att om $(m,n) = 1$, så är $\phi(mn) = \phi(m)\phi(n)$.

I 22 Bestäm alla element i a) $\mathbb{Z}_{17}$, b) $\mathbb{Z}_{15}$ som satisfierar ekvationen $\overline{12}.x = \overline{9}$.

I 23 Bestäm alla element i a) $\mathbb{Z}_{11}$, b) $\mathbb{Z}_{13}$ som satisfierar ekvationen $x^2 = -\overline{1}$.

I 24 Bestäm alla element i $\mathbb{Z}_{15}$ som satisfierar ekvationen $x^2 = \overline{1}$.

* avsevärt svårare än övriga uppgifter i denna avdelning.

Svar

I 1 a) 1-1 men inte på b) 1-1 och på c) varken 1-1 eller på.

I 2 a) varken på eller 1-1 b) på men inte 1-1

c) 1-1 men inte på d) både 1-1 och på.

I 3 $f \circ g$ betyder g först och sedan f:

a) f på, men inte nödvändigt g: ta t.ex. $g: \mathbb{R} \to \mathbb{R}$ med $g(x) = |x|$ och $f: \mathbb{R} \to \mathbb{R} \setminus \{0\}$ med $f(x) = x^2$.

b) g 1-1 men inte nödvändigt f: ta t.ex. $g: \mathbb{R}_+ \cup \{0\} \to \mathbb{R}$ med $g(x) = x^2$ och $f: \mathbb{R} \to \mathbb{R}$ med $f(x) = |x|$.

I 4 c) $f: \mathbb{Z}_+ \to \mathbb{Z}_+$ given av att $f(n) = n+1$ är 1-1 men inte på;
$g: \mathbb{Z}_+ \to \mathbb{Z}_+$ given av att $g(n) = \left[\frac{n}{10}\right]$ = heltalsdelen av $\frac{n}{10}$ är på men inte 1-1

I 5 Låt E(a) beteckna den ekvivalensklass som bestäms av a för $a \in S$.

a) nej b) ja; $E(a) = \{a + \ln q \; ; \; q \in \mathbb{Q}\}$

c) ja; $E(a) = \{b \in \mathbb{C} \setminus \{0\}$; arg a = arg b$\}$ = halvstrålen från origo genom a i det komplexa talplanet.

d) nej e) nej f) ja; $E(f) = \{f + r \; ; \; r \in \mathbb{R}\}$

g) ja; $E(A) = \{B \; ; \; \det(B) = \det(A)\}$ h) nej.

I 6 E(1) = alla jämna kvadrater, E(2) = alla positiva heltal av formen 2. jämn kvadrat.

I 7 a) 1 b), c) $r_n = (360,539) = 179.539 - 268.360$

I 8 $7 = 20.287 - 7.819$

I 9 a) s = -23, t = 2 t.ex. b) finns inga s och t

I 10 c) $(a,b) \mid c$

I 11 a) 5 b) 6 c) 6 d) 0

I 14 a) falskt, ta t.ex. a = 2, b = 5 b) och c) sanna.

I 15

+	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

•	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

+	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

•	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

I 16 a) ja b) nej

I 17 $\overline{3}.\overline{b} \neq \overline{1}$ för alla $\overline{b} \in \mathbb{Z}_6$ enl. tabellen i I 15.

I 18 a) (i) och (iii) saknar lösning, (ii) har lösningen x = $\overline{7}$

b) (i) x = $\overline{6}$ (ii) x = $\overline{4}$ (iii) x = $\overline{9}$

c) (i), (ii) saknar lösning, (iii) x = $\overline{5}$.

I 19 a) $\overline{1},\overline{3},\overline{5},\overline{7}$ b) $\overline{1},\overline{2},\overline{4},\overline{5},\overline{7},\overline{8}$ c) $\overline{1},\overline{3},\overline{7},\overline{9}$

I 20 a) (a,n) = 1

I 21 a) 2,2,4,2,6,4,6,4,10,4,12,6,8,8,16,6,18,8.

b) p -1

I 22 a) $\overline{5}$ b) $\overline{2},\overline{7},\overline{12}$

I 23 a) finns inga b) $\overline{5}$ och $\overline{8}$

I 24 $\overline{1},\overline{4},\overline{11},\overline{14}$.

Ledningar.

I 1 $f:S \to T$ på $\Leftrightarrow$ (ekvationen $t = f(x)$ har lösning för varje $t \in T$).

$f:S \to T$ 1-1 $\Leftrightarrow$ ($f(x) = f(y) \Rightarrow x = y$ för alla $x,y \in S$).

I 4 Låt n = antalet element i S. Hur många element i S är bilder under f om f är 1-1?

I 9 a) jfr I 7c) b) Visa att vänsterledet $7s + 91t$ har en divisor > 1.

I 10 a) $(a,b) \mid (ax + by)$ för alla $x,y \in \mathbb{Z}$ b) jfr I 7c)

c) jfr ledningen till a). För tillräckligheten, dividera båda leden med (a,b) och använd b).

I 12 $n^3 - n = n(n-1)(n+1)$.

I 13 Betrakta $21^n + 7^n$ modulo 14.

I 19 Pröva!

I 20 jfr I 10. $\bar{a} \cdot x = \bar{1}$ är ju ekvivalent med en ekvation $ax = 1 + ny$ för $x,y \in \mathbb{Z}$.

I 21 c) $(a,p^k) \neq 1 \Leftrightarrow a = np$ för något $n \in \mathbb{Z}$. Hur många heltal av den formen finns bland heltalen från 1 till p^k?

d) Skriv upp talen från 1 till mn i en kvadrat med n rader och m kolonner:

1	2	.	.	.	m
m+1	m+2	.	.	.	2m
.	.	.	.	.	.
(n-1)m + 1	.	.	.	.	mn

Elementen i en fix kolonn har alla samma största gemensamma divisor med m. De n elementen i en kolonn är parvis inkongruenta modulo n, så varje restklass modulo n har precis en representant i kolonnen.

I 22 Pröva! Observera att en förstagradsekvation i $\mathbb{Z}_n$ kan ha fler än en lösning.

I 23 Pröva! Tänk på att $\bar{a}^2 = (-\bar{a})^2$. Bara hälften av elementen i $\mathbb{Z}_n$ behöver alltså prövas.

Lösningar.

I 3 Låt $f:T \to U$ och $g:S \to T$.

a) $f \circ g$ på $\Rightarrow$ till varje $u \in U$ finns $s \in S$ så att $u = f \circ g(s) = f(g(s)) \Rightarrow$ till varje $u \in U$ finns $t \in T$ så att $u = f(t)$ (ta $t = g(s)$) $\Rightarrow$ f på.

Betrakta $f:\mathbb{R} \to \mathbb{R}\setminus\{0\}$ med $f(x) = x^2$, $g:\mathbb{R} \to \mathbb{R}$ med $g(x) = |x|$. g är inte på trots att $f \circ g$ är på.

b) $g(x) = g(y) \Rightarrow f \circ g(x) = f \circ g(y) \Rightarrow x = y$, om $f \circ g$ 1-1. Alltså är g 1-1.

För att se att f inte nödvändigt 1-1, betrakta $g:\mathbb{R}\setminus\{0\} \to \mathbb{R}$ med $g(x) = x^2$ och $f:\mathbb{R} \to \mathbb{R}$ med $f(x) = |x|$. Då är $f \circ g:\mathbb{R}\setminus\{0\} \to \mathbb{R}$ given av att $f \circ g(x) = x^2$, alltså 1-1.

I 4 Sätt n = antalet element i S.

a) f på $\Rightarrow$ antalet bildelement = n. Om två av elementen i S avbildades på samma element, så vore antalet bildelement $\leq n-1$. Alltså är f 1-1, om f är på.

b) f 1-1 $\Rightarrow$ olika element har olika bilder $\Rightarrow$ antalet element i bilden = n $\Rightarrow$ bildmängden = S $\Rightarrow$ f på.

I 7 a) $539 = 1 \cdot 360 + 179$

$360 = 2 \cdot 179 + 2$

$179 = 89 \cdot 2 + 1$

Sista icke-försvinnande resten = $1 = (360,539)$.

b) $n = 3$; $r_3 = 1 = 179 - 89 \cdot 2 = r_1 - 89 \cdot r_2 = r_1 - 89(360 - 2r_1) = 179r_1 - 89 \cdot 360 = 179(539 - 360) - 89 \cdot 360 = 179 \cdot 539 - 268 \cdot 360$

c) ur b) fås $s = -268$, $t = 179$.

I 10 a) Antag $as + bt = 1$ för några $s,t \in \mathbb{Z}$. $(a,b)|a$ och $(a,b)|b \Rightarrow (a,b)|(as + bt) \Rightarrow (a,b)|1 \Rightarrow (a,b) = 1$

b) Antag $(a,b) = 1$. Om man går baklänges i Euklides' algoritm för a och b (jfr I 7b)), så får man $1 = (a,b) = as + bt$ för några $s,t \in \mathbb{Z}$. Ta $x = s$, $y = t$.

c) Om $as + bt = c$ för några $s,t \in \mathbb{Z}$, så $(a,b) \mid (as + bt) = c$. Omvänt, om $(a,b) \mid c$ så sätt $a = (a,b)\cdot a_1$, $b = (a,b)\cdot b_1$, $c = (a,b)\cdot c_1$. Vi får ekvationen $a_1x + b_1y = c_1$ med $(a_1,b_1) = 1$. Enligt b) finns $s,t \in \mathbb{Z}$ så att $a_1s + b_1t = 1$. Multiplikation av båda leden med c_1 ger lösningen $x = sc_1$, $y = tc_1$ till ekvationen $ax + by = c$.

I 18 a)

x	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{9}$
$\bar{2}\cdot x$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{8}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{8}$
$\bar{3}\cdot x$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{9}$	$\bar{2}$	$\bar{5}$	$\bar{8}$	$\bar{1}$	$\bar{4}$	$\bar{7}$
$\bar{5}\cdot x$	$\bar{0}$	$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{0}$	$\bar{5}$

Av tabellen framgår att ekvationerna $\bar{2}\cdot x = \bar{1}$ och $\bar{5}\cdot x = \bar{1}$ saknar lösning samt att ekvationen $\bar{3}\cdot x = \bar{1}$ har lösningen $x = \bar{7}$.

I 21 d) Skriv heltalen från 1 till mn i en kvadrat med n rader och m kolonner:

1	2	.	.	m
m+1	m+2	.	.	2m
.	.	.	.	.
(n-1)m+1	.	.	.	nm

Vi skall stryka alla tal a av dessa för vilka $(a,mn) \neq 1$. $(a,mn) \neq 1 \iff ((a,m) \neq 1$ eller $(a,n) \neq 1)$. Varje kolonn representerar en restklass modulo m, så alla tal som står i en kolonn har samma största gemensamma divisor med m. Vi stryker då först alla kolonner med element a sådana att $(a,m) \neq 1$. Det återstår $\phi(m)$ kolonner där alla element är relativt prima till m. Betrakta en sådan kolonn. Den har n stycken element: $b_i = b + (i-1)m$. $b_i \equiv b_j \pmod{m} \Rightarrow b_i \not\equiv b_j \pmod{n}$ om $i \neq j$ eftersom $(m,n) = 1$ och $|b_i - b_j| < mn$. De n elementen i en

kolonn bildar alltså en fullständig familj av representanter för restklasserna modulo n. Av dessa n element i en kolonn har alltså $\phi(n)$ stycken s.g.d. = 1 med n medan de övriga har s.g.d. > 1 med n. De senare stryks. I var och en av de $\phi(m)$ kolonner som inte strukits finns $\phi(n)$ element kvar. Dessa $\phi(m)\phi(n)$ är relativt prima till både m och n, alltså också till mn.

I 23 a)

x	$\overline{0}$	$\pm\overline{1}$	$\pm\overline{2}$	$\pm\overline{3}$	$\pm\overline{4}$	$\pm\overline{5}$
x^2	$\overline{0}$	$\overline{1}$	$\overline{4}$	$\overline{9}$	$\overline{5}$	$\overline{3}$

Det finns alltså inget $x \in \mathbf{Z}_{11}$ så att $x^2 = -\overline{1} = \overline{10}$.

Grupper

GA 1 M är en mängd och $*$ en komposition på M (dvs till varje par a,b i M ordnar $*$ ett element $a * b$ i M). Ange för vart och ett av nedanstående exempel vilka av följande egenskaper som gäller:

(i) $*$ är associativ i M (ii) $*$ är kommutativ i M

(iii) M har neutralt element för $*$

(iv) elementen i M har invers under $*$ (om inte alla element har invers, så ange vilka som har det).

(iv) behöver förstås undersökas bara om (iii) visats gälla.

a) $M = \{a_1, a_2, a_3, a_4\}$, $*$ definieras genom multiplikationstabellen:

$*$	a_1	a_2	a_3	a_4
a_1	a_2	a_1	a_3	a_4
a_2	a_1	a_4	a_2	a_3
a_3	a_3	a_2	a_4	a_1
a_4	a_4	a_3	a_1	a_1

Tabellen betyder:

$a_i * a_j$ = det element som står i a_i:s rad och a_j:s kolonn

b) $M = \mathbb{Q}$; $a * b = a + b - ab$ c) $M = \mathbb{Q}$, $a * b = a - b + ab$

d) M = de icke-negativa reella talen, $a * b = \min(a,b)$

e) M = - " - , $a * b = \sqrt{a^2 + b^2}$

f) M = delmängderna av $\mathbb{R}$, $*$ = unionsbildning

g) $M = \{A, B, C, D\}$

$*$	A	B	C	D
A	A	A	A	A
B	B	B	B	B
C	C	C	C	C
D	D	D	D	D

h) $M = \{1, 2, 3, 4\}$

$*$	1	2	3	4
1	1	2	3	4
2	2	1	4	3
3	3	4	1	2
4	4	2	3	1

GA 2 Vilka av följande mängder M med operationer $*$ bildar en grupp?

a) $M = \mathbb{Z}$, $a * b = a + b + 10$

b) $M = \{a/b \in \mathbb{Q};\ b \text{ udda}\}$, $*$ = addition

c) $M = \{a/b \in \mathbb{Q};\ b \text{ udda},\ a \neq 0\}$, $*$ = multiplikation

d) $M = \mathbb{Q} \setminus \{0\}$, $a * b = a/b$

e) $M = \{z \in \mathbb{C};\ \mathrm{Re}\ z = 4\ \mathrm{Im}\ z\}$, $*$ = addition

f) $M = \{z \in \mathbb{C};\ \mathrm{Re}\ z = \mathrm{Im}\ z + 4\}$, $*$ = addition

g) $M = \{\overline{1},\overline{5},\overline{7},\overline{11}$ modulo 12$\}$, $*$ = restklassmultiplikation

h) $M = \{\overline{2},\overline{4},\overline{8},\overline{10}$ modulo 12$\}$, $*$ = - " -

i) $M = \{\overline{2},\overline{4},\overline{6},\overline{8}$ modulo 10$\}$, $*$ = - " -

k) $M = \{z \in \mathbb{C};\ z^n = 1\}$ (n fixt), $*$ = multiplikation

l) $M = \{$funktionerna $f_1, f_2, f_3: \mathbb{R} \setminus \{0,1\} \to \mathbb{R} \setminus \{0,1\}$; $f_1(x) = x$

$f_2(x) = 1/(1 - x)$, $f_3(x) = (x - 1)/x\}$,

$*$ = funktionssammansättning

m) $M =$ {inverterbara 2 x 2-matriser}, $*$ = matrismultiplikation

n) $M = \{\begin{pmatrix} a & b \\ 0 & a \end{pmatrix};\ a,b \in \mathbb{Z},\ a \neq 0\}$, $*$ = - " -

GA 3 Vilka av följande multiplikationstabeller representerar grupper?

a)

$*$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	b	a
d	d	b	a	c

b)

$*$	a	b	c	d
a	c	d	a	b
b	d	c	b	a
c	a	b	c	d
d	b	a	d	c

GA 4 Visa att nedanstående tabell på ett entydigt sätt kan fullbordas så att den blir en multiplikationstabell för en grupp.

	e	a	b	c
e	e	a	b	c
a	a	e	.	.
b	b	.	e	.
c	c	.	.	e

GA 5 Låt $M = \mathbb{Z} \times \mathbb{Z}$ (= mängden av ordnade par av heltal) och låt $(a,b) * (c,d) = (a + d, b + d)$.

a) Visa att $*$ är associativ.

b) Finn ett ordnat par ε som är en högeridentitet (dvs $\alpha * \varepsilon = \alpha$

för alla $\alpha \in M$) och sådan att för varje $\alpha \in M$ finns β så att

$\beta * \alpha = \varepsilon$ (dvs β är vänsterinvers till α)

c) Är M en grupp under $*$?

GA 6 Visa att i en grupp med det neutrala elementet e gäller att $a^2 = a$ medför $a = e$.

GA 7 Visa att i en grupp gäller att $(a^{-1}b\ a)^k = a^{-1}\ b\ a$ om och endast om $b^k = b$.

GA 8 Visa att om för alla element a,b i en grupp gäller att $a^2\ b^2 = (ab)^2$, så är gruppen abelsk.

GA 9 'Lös' för att få x uttryckt i a,b och c:

a) xaxaba = xbc b) $ax^2 = b$ och $x^3 = e$ c) $x^5 = e$ och $x^3 = a$.

GA 10 Bestäm alla delgrupper av den additiva gruppen $\mathbb{Z}_{18}$.

GA 11 I vilka delgrupper av $\mathbb{Z}_{12}$ under addition ingår 8?

GA 12 Ange en delgrupp H av den additiva gruppen $\mathbb{R}$ sådan att $H \neq \mathbb{R}$ och $\pi \in H$.

GA 13 Är $\{\begin{pmatrix}1 & k\\0 & 1\end{pmatrix}\ ;\ k \in \mathbb{Z}\}$ en delgrupp av gruppen av inverterbara 2 x 2-matriser under matrismultiplikation?

GA 14 Låt a vara ett fixt element i en grupp G. Visa att $N_a = \{x \in G;\ ax = xa\}$ är en delgrupp av G.

GA 15 Visa att följande 6 matriser bildar en grupp med matrismultiplikation som operation. Bestäm elementens ordningar.

$$\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}, \begin{pmatrix}-1 & 1\\-1 & 0\end{pmatrix}, \begin{pmatrix}0 & -1\\1 & -1\end{pmatrix}, \begin{pmatrix}1 & 0\\1 & -1\end{pmatrix}, \begin{pmatrix}0 & -1\\-1 & 0\end{pmatrix}, \begin{pmatrix}-1 & 1\\0 & 1\end{pmatrix}.$$

GA 16 Visa att $\{\overline{1},\overline{2},\overline{3},\overline{4},\overline{5},\overline{6}$ modulo $7\}$ bildar en grupp under restklassmultiplikation. Bestäm elementens ordningar. Är gruppen cyklisk?

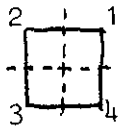
GA 17 Betrakta $\mathbb{Z}_3 \times \mathbb{Z}_4$, dvs mängden av ordnade par (a,b), där $a \in \mathbb{Z}_3$ och $b \in \mathbb{Z}_4$. Inför kompositionen (a,b)(c,d) = (a+c, b+d) där additionerna i högra ledet är restklassaddition i $\mathbb{Z}_3$ resp. $\mathbb{Z}_4$.

a) Visa att $\mathbb{Z}_3 \times \mathbb{Z}_4$ med denna komposition är en abelsk grupp.

b) Vilken ordning har denna grupp?

c) Är gruppen cyklisk?

GA 18 Symmetri av en n-hörning = avbildning av n-hörningen på sig själv så att avstånd bevaras. Speciellt avbildas hörn på hörn. Mängden av symmetrier av en n-hörning bildar en grupp under funktionssammansättning (visa!). Symmetrierna av en kvadrat är följande:



I = identiska avbildningen — V = spegling i vertikala axeln

R_1 = rotation 1/4 varv motsols — H = " i horisontella axeln

R_2 = " 1/2 " " — D_1 = " i diagonalen 1-3

R_3 = " 3/4 " " — D_2 = " " " 2-4

Vi får följande multiplikationstabell för gruppen av symmetrier av en kvadrat

	I	R_1	R_2	R_3	V	H	D_1	D_2
I	I	R_1	R_2	R_3	V	H	D_1	D_2
R_1	R_1	R_2	R_3	I	D_1	D_2	H	V
R_2	R_2	R_3	I	R_1	H	V	D_2	D_1
R_3	R_3	I	R_1	R_2	D_2	D_1	V	H
V	V	D_2	H	D_1	I	R_2	R_3	R_1
H	H	D_1	V	D_2	R_2	I	R_1	R_3
D_1	D_1	V	D_2	H	R_1	R_3	I	R_2
D_2	D_2	H	D_1	V	R_3	R_1	R_2	I

(Operationerna appliceras till höger så att t.ex. VH betyder att V tas först och sedan H)

a) Bestäm alla delgrupper av denna grupp.

b) Bestäm alla cykliska delgrupper av denna grupp.

c) Vilken delgrupp genereras av $\{V,H\}$, av $\{V,H,D_1\}$?

d) Skriv upp alla sidoklasser (vänster och höger) till delgrupperna

$\{I,V\}$, $\{I,R_2\}$, $\{I,V,H,R_2\}$.

e) Vilka av dessa delgrupper är normala?

f) Gör multiplikationstabell för faktorgruppen modulo $\{I,R_2\}$.

GA 19 Restklasserna $\overline{1},\overline{2},\overline{4},\overline{7},\overline{8},\overline{11},\overline{13},\overline{14}$ modulo 15 bildar en grupp G under restklassmultiplikation och $H = \{\overline{1},\overline{4}\}$ är en delgrupp. Skriv upp sidoklasserna till H i G och gör multiplikationstabell för G/H.

GA 20 Visa att H = {2 x 2-matriser med determinant > 0} är en delgrupp av index 2 av gruppen av inverterbara 2 x 2-matriser under matrismultiplikation.

GA 21 Visa att mängden {2 x 2-matriser med determinant = 1} är en normal delgrupp av gruppen av inverterbara 2 x 2-matriser under matrismultiplikation.

GA 22 Visa att en delgrupp av index 2 är normal.

GA 23 Låt $G = \{(a,b);\ a,b \in \mathbb{R},\ b \neq 0\}$. Definiera en operation i G genom $(a,b) * (c,d) = (a + bc,\ bd)$.

a) Visa att G är en grupp under $*$.

b) Visa att $N = \{(a,1);\ a \in \mathbb{R}\}$ är en normal delgrupp i G

c) Visa att $\phi\colon G \to \mathbb{R}\setminus\{0\}$ given av att $\phi(a,b) = b$ är en grupphomomorfism

d) Bestäm ϕ:s kärna. e) Ange en grupp som är isomorf med G/N.

GA 24 Vilka av följande avbildningar är grupphomomorfismer? Bestäm i förekommande fall kärnan.

a) $\phi\colon (\mathbb{R},+) \to (\mathbb{R},+)$ med $\phi(x) = x^2$

b) $\phi\colon (\mathbb{R},+) \to (\mathbb{R},+)$ med $\phi(x) = 2x$

c) $\phi\colon (\mathbb{R}_+,\cdot) \to (\mathbb{R}_+,\cdot)$ med $\phi(x) = x^2$

d) $\phi\colon (\mathbb{R}_+,\cdot) \to (\mathbb{R}_+,\cdot)$ med $\phi(x) = 2x$

e) $\phi\colon (\mathbb{R},+) \to (\mathbb{R}_+,\cdot)$ med $\phi(x) = 2^x$

f) $\phi\colon (\mathbb{R},+) \to (\mathbb{Z},+)$ med $\phi(x)$ = heltalsdelen av x (= det största heltal som är $\leq x$)

g) ϕ: $(\mathbb{Z}_{18},+) \to (\mathbb{Z}_{18},+)$ med $\phi(x) = 6x$.

h) G = gruppen av inverterbara 2 x 2-matriser under multiplikation

ϕ: $G \to (\mathbb{R}\setminus\{0\}, \cdot)$ med $\phi(A) = \det(A)$.

i) $G = \{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$; $a,b \in \mathbb{R}$, $a \neq 0\}$ under multiplikation

ϕ: $G \to (\mathbb{R}\setminus\{0\}, \cdot)$ med $\phi(\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}) = a$.

GA 25 a) Bestäm en homomorfism $\neq 0$ från $(\mathbb{Z}_8,+)$ till $(\mathbb{Z}_4,+)$.

b) " " - " - " - $(\mathbb{Z}_8,+)$ " $(\mathbb{Z}_5,+)$.

GA 26 Låt G vara en grupp och låt f:G → G vara given av att $f(x) = x^{-1}$. Under vilka villkor på G är f en homomorfism? En automorfism?

GA 27 Följande 4 mängder av restklasser är grupper under restklassmultiplikation. Vilka grupper är isomorfa?

$G_1 = \{\overline{1}, \overline{2}, \overline{3}, \overline{4} \mod 5\}$

$G_2 = \{\overline{1}, \overline{3}, \overline{5}, \overline{7} \mod 8\}$

$G_3 = \{\overline{1}, \overline{3}, \overline{7}, \overline{9} \mod 10\}$

$G_4 = \{\overline{1}, \overline{5}, \overline{7}, \overline{11} \mod 12\}$

GA 28 Visa att det finns en isomorfism av $(\mathbb{Z}_6,+)$ på gruppen av element $\neq \overline{0}$ i $\mathbb{Z}_7$ under restklassmultiplikation, sådan att bilden av $\overline{1}$ i den första gruppen är elementet $\overline{3}$ i den senare.

GA 29 a) Visa att $\{m + ni;\ m,n \in \mathbb{Z},\ i^2 = -1\}$ under addition resp. $\{2^m3^n;\ m,n \in \mathbb{Z}\}$ under multiplikation är grupper.

b) Visa att grupperna i a) är isomorfa.

GA 30 a) Visa att $H = \{z \in \mathbb{C};\ \mathrm{Re}\ z = 0\}$ är en delgrupp av $(\mathbb{C},+)$.

b) Visa att $\mathbb{C}/H = (\mathbb{R},+)$ genom att definiera en homomorfism av $\mathbb{C}$ på $\mathbb{R}$ med H som kärna.

GA 31 $(\mathbb{Z}_5,+)$ är en cyklisk grupp.

a) Visa att en homomorfism $\mathbb{Z}_5 \to \mathbb{Z}_5$ är bestämd så snart bilden av $\overline{1}$ är bestämd.

b) Visa genom att undersöka vad $\overline{1}$ kan avbildas på, att det finns 4 automorfismer av $\mathbb{Z}_5$.

c) Visa att dessa 4 automorfismer bildar en cyklisk grupp under funktionssammansättning.

d) Undersök på samma sätt hur många automorfismer av $(\mathbb{Z}_6,+)$ det finns.

GA 32 a) Visa att en homomorfism $\phi:(\mathbb{Q},+) \to (\mathbb{Q},+)$ är bestämd så snart bilden av 1 är bestämd, nämligen så att $\phi(x) = x\phi(1)$ för $x \in \mathbb{Q}$.

b) Visa att avbildningen {automorfismer av $(\mathbb{Q},+)$} $\to (\mathbb{Q}\setminus\{0\},.)$ som avbildar ϕ på $\phi(1)$ är en gruppisomorfism.

GA 33 Gruppen G' kallas homomorf bild av gruppen G om det finns en grupphomomorfism av G på G'.

a) Visa att en homomorf bild av en cyklisk grupp själv är cyklisk.

b) Vilka grupper är homomorfa bilder av $(\mathbb{Z}_{17},+)$ resp. $(\mathbb{Z}_{18},+)$?

GA 34 $\{1,-1,i,-i\}$ $(i^2 = -1)$ är en grupp under multiplikation. Visa att den är homomorf bild av $(\mathbb{Z},+)$ och ange motsvarande kärna.

GA 35 Uttryck var och en av följande element i S_7 som en produkt av disjunkta cykler:

a) $(1,2,3)(1,6,5,4,3)$ b) $(2,1,3,4,5,6)(1,7,2)$

c) $(1,7,2)(2,1,3,4,5,6)$ d) $(4,2,1,5)(3,4,2,6)(5,6,7,1)$

e) $(1,2,3,4)(1,2,4)(3,1,2,7)(5,6)$ f) $(1,2)(1,3)(1,4)(1,5)(1,6)(1,7)$

GA 36 Bestäm cykelstrukturen för $a^2,\ldots,a^6$ om $a = (1,2,3,4,5,6,7,8,9,10,11,12)$

GA 37 a) Visa att $(a_1,a_2,\ldots,a_n)^{-1} = (a_n,\ldots,a_2,a_1)$

b) Bestäm inverserna till permutationerna i uppgift GA 35.

GA 38 a) Visa att cykeln $(a_1,a_2,\ldots,a_n) = (a_1,a_2)(a_1,a_3)\ldots(a_1,a_n)$

b) Bestäm med hjälp av a) för vilka m en m-cykel är en jämn permutation.

c) Vilka av permutationerna i GA 35 är udda?

GA 39 a) Visa att mängden $V = \{(1),(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}$ är en delgrupp av S_4.

b) Skriv upp alla vänster- resp. högersidoklasser till V i S_4. Är V normal i S_4?

c) Elementen (1),(1,2),(1,3),(2,3),(1,2,3),(1,3,2) ligger alla i olika sidoklasser till V. Använd detta för att konstruera en isomorfi mellan S_4/V och S_3.

GB 1 Låt $M = \{x \in R;\ x \neq 0,1\}$. $f,g:M \to M$ ges av att $f(x) = \frac{1}{x}$ och $g(x) = \frac{1}{1-x}$. Bestäm den grupp som genereras av f och g med funktionssammansättning som operation.

GB 2 a) Visa att $Z_n^* = \{\bar{a} \in Z_n;\ (a,n) = 1\}$ är en grupp under restklassmultiplikation.

b) Vad är ordningen av Z_n^*?

c) Skriv upp elementen i Z_{18}^*. Är Z_{18}^* cyklisk?

d) Visa att Z_{10}^* är isomorf med en delgrupp av Z_{15}^*.

GB 3 a) Låt G vara en abelsk grupp. Visa att mängden T av element av ändlig ordning bildar en delgrupp av G.

b) Bestäm T om G är gruppen av reella tal $\neq 0$ under multiplikation.

c) " - " - " - komplexa " - " - " -

d) Visa att i gruppen av inverterbara 2 x 2-matriser under matrismultiplikation har elementen av formen $\begin{pmatrix} 1 & a \\ 0 & -1 \end{pmatrix}$ ändlig ordning.

e) Visa med hjälp av d) att påståendet i a) inte nödvändigt är sant i en icke-abelsk grupp G.

GB 4 Låt G vara en grupp med neutralt element e och låt $a,b \in G$.

Visa att följande relationer var och en medför $ab = ba$:

a) $ba^{-1}b^{-1}a = e$ b) $aba^2 = e$ c) $abab^2 = e$.

Visa genom att studera en lämplig grupp att relationen $(ab)^2 = (ba)^2$ ej nödvändigt medför $ab = ba$.

GB 5 a) Visa att om $a^2 = e$ för varje a i en grupp G, så är G abelsk.

b) Visa också att ordningen av G är en potens av 2, om ordningen är ändlig.

GB 6 Låt o(a) vara ordningen av elementet a i G. Visa att om $a^m = e$, så är $o(a) \mid m$.

GB 7 G är en cyklisk grupp av ordning m med generator x. Visa att x^k är en generator för G om och endast om $(m,k) = 1$.

GB 8 Låt G vara en grupp och a,b element i G.

a) Visa att a och a^{-1} har samma ordning.

b) Visa att ab och ba har samma ordning.

GB 9 G är en ändlig grupp av jämn ordning. Visa att det finns minst ett element $x \neq e$ i G sådant att $x = x^{-1}$.

GB 10 Visa att om en grupp G har ett enda element a av ordning 2 så är $ax = xa$ för alla $x \in G$.

GB 11 Visa att varje delgrupp av en cyklisk grupp själv är cyklisk.

GB 12 Låt G vara en grupp med delgrupperna H och K av ordning m resp. n. Visa att om $(m,n) = 1$, så är $H \cap K = \{e\}$

GB 13 Låt G vara en grupp.

a) Visa att mängden $Z_G = \{a \in G;\ ax = xa \text{ för alla } x \in G\}$ är en normal delgrupp av G (den kallas centrum av G).

b) Vad är centrum av en abelsk grupp?

c) Bestäm centrum av S_3.

d) Bestäm centrum av gruppen i GA 18.

GB 14 Låt G vara en grupp och H en delgrupp av G. Sätt för $g \in G$ $gHg^{-1} = \{ghg^{-1};\ h \in H\}$.

a) Visa att gHg^{-1} är en delgrupp av G med samma ordning som H.

b) Visa att om H är den enda delgruppen av ordning o(H) så är H normal i G.

GB 15 a) Visa att den grupp som genereras av matriserna

$$A = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \quad \text{och } B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad (i^2 = -1)$$

under matrismultiplikation har ordning 8 och är icke-abelsk.

b) Bestäm elementens ordningar.

c) Bestäm alla delgrupper.

d) Visa att alla delgrupper är normala.

(Detta exempel visar att omvändningen till påståendet (G abelsk $\Rightarrow$ alla delgrupper är normala) inte är sann.)

GB 16 Om N är normal delgrupp av G och $a \in G$, visa att ordningen av Na i G/N är en delare till o(a).

GB 17 N är en normal delgrupp i G och $a \in G$. Visa att om o(a) och o(G/N) är relativt prima, så ligger a i N.

GB 18 Ge ett exempel på en icke abelsk grupp G med en abelsk normal delgrupp N sådan att G/N är abelsk.

GB 19 Det reella vektorrummet av dimension n, $\mathbb{R}^n$, bildar en grupp under addition. Visa att $(\mathbb{R}^3,+)$ avbildas homomorft på $(\mathbb{R}^2,+)$ genom $(x,y,z) \to (x+y+z, 2x-y+3z)$. Bestäm också kärnan.

GB 20 Betrakta mängden $M = \{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} ; a \in \mathbb{R}\}$. Visa att M är en grupp under matrismultiplikation, isomorf med $(\mathbb{R},+)$.

GB 21 Visa att $(\mathbb{R},+)$ och $(\mathbb{R}_+,.)$ är isomorfa grupper.

GB 22 Visa att två cykliska grupper av samma ordning är isomorfa.

GB 23 Visa att gruppen i GA 2a) är isomorf med $(\mathbb{Z},+)$.

GB 24 a) Visa att om $f:G \to G'$ är en gruppisomorfism, så har x och f(x) samma ordning.

b) Hur förhåller sig ordningarna av x och f(x) till varandra om f är en homomorfism?

GB 25 G är en cyklisk grupp av ordning 58. Bestäm varje element i G som av samtliga automorfismer av G avbildas på sig självt.

GB 26 Visa att grupperna $\mathbb{Z}_{15}^*$ och $\mathbb{Z}_{24}^*$ (för definition av $\mathbb{Z}_n^*$, se uppgift GB 2) vardera har åtta element och undersök om de är isomorfa.

GB 27 a) Visa att $T = \{z \in \mathbb{C};\ |z| = 1\}$ är en delgrupp av $(\mathbb{C} \setminus \{0\}, .)$.

b) Visa att $\mathbb{C} \setminus \{0\}/T \simeq (\mathbb{R}_+, .)$.

GB 28 T som i föregående uppgift. Visa att $T \simeq \mathbb{R}/\mathbb{Z}$ där operationen på $\mathbb{R}$ är addition.

GB 29 Låt G vara gruppen $\{e,a,b,ab;\ a^2 = b^2 = e,\ ba = ab\}$.
Bestäm gruppen av automorfismer av G.

GB 30 a) Visa att det finns sex inre automorfismer av S_3.

b) Visa att det finns högst sex automorfismer av S_3.

c) Visa att automorfismgruppen av S_3 är isomorf med S_3.

GB 31 $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ (dvs mängden av tripler (a,b,c) med $a,b,c \in \mathbb{Z}_2$) bildar en grupp under restklassaddition komponentvis. Finns det någon automorfism $\neq$ identiteten av G?

GB 32 Låt G vara gruppen $\{e,a,a^2,a^3,b,ab,a^2b,a^3b;\ o(a) = 4,$ $o(b) = 2,\ ba = a^3b\}$. Visa att G har åtta automorfismer och att fyra av dessa är inre automorfismer.

GB 33 a) Vad är ordningen av en k-cykel i S_n $(n \geq k)$?

b) Vad är ordningen av en produkt av disjunkta cykler av längderna $m_1, m_2, \ldots, m_k$?

GB 34 Bestäm antalet element av ordning 5 samt antalet element av ordning 3 i S_6. Kontrollera resultaten med hjälp av satsen: om n är en divisor till gruppens ordning, så är antalet element x för vilka $x^n = e$ en multipel av n (neutrala elementet e är ett av dessa).

GB 35 I S_5 betraktas elementen $a = (1,2,3,4)$ och $b = (1,2)(4,5)$.

a) Skriv elementen ab, a^2b, a^3b som produkter av disjunkta cykler. Verifiera att $aba^2ba^3b = e$ (den identiska permutationen).

b) Uttryck bab, ba^2b, ba^3b som produkter som inte innehåller mer än en faktor b.

c) Låt H vara den delgrupp av S_5 som genereras av a och b. Visa att varje element i H kan skrivas på formen a^m eller a^mba^n, där m = 0,1,2 eller 3 och n = 0,1,2 eller 3.

GB 36 G är en grupp, a och b två element i G.

a) Ge ett exempel där o(a) = 2, o(b) = 3 och o(ab) = 4.

b) Bestäm o(ab) om o(a) = 4, o(b) = 6 och G är abelsk.

GB 37 a) I gruppen A_n ($n \geq 4$) av jämna permutationer av 1,2,...,n bildar de permutationer som avbildar a på sig självt en delgrupp H_a. Visa det.

b) Visa att delgrupperna H_a (a = 1,2,...,n) är isomorfa.

GB 38 Låt ρ och τ beteckna de permutationer i S_{10} som överför (1,2,3,4,5,6,7,8,9,10) i (2,1,4,5,3,7,8,9,10,6) resp. (1,2,4,3,5,7,8,9,10,6). Låt H vara den delgrupp som genereras av ρ och τ.

a) Skriv ρ och τ som produkter av disjunkta cykler.

b) Visa med hjälp av a) att H genereras av fyra element av ordningarna 2,2,3,5.

c) Bestäm ordningen av H.

GB 39 a) Visa att för $\tau \in S_n$ är $\tau^{-1}(a_1,a_2,..,a_k)\tau = (\tau(a_1),\tau(a_2),..,\tau(a_k))$.

b) Givet x = (1,3,4)(2,6) och y = (1,4)(2,3,5) i S_6 finn $a \in S_6$ så att $y = a^{-1}xa$

c) Visa att det inte finns något $a \in S_5$ så att $a^{-1}(1,2)(3,5)a = (3,5,2,4)$.

d) Visa att $y = a^{-1}xa$ för något $a \in S_n$ om och endast om x och y

har cykeluppdelningar av samma typ (dvs. cykeluppdelningarna innehåller lika många cykler av given längd).

GB 40 a) Hur kan cykelframställningen se ut för ett element av ordningen 5 i S_5?

b) Visa att S_5 inte har någon normal delgrupp av ordning 5.

c) Visa (gärna med användande av det föregående) att S_4 inte kan vara homomorf bild av S_5.

GC 1 Visa att det finns precis två icke-isomorfa typer av grupper av ordning 4.

GC 2 Visa att det finns precis två icke-isomorfa typer av grupper av ordning 6.

GC 3 Visa att det finns precis två icke-isomorfa typer av grupper av ordning 10.

GC 4 I en grupp G gäller följande relationer för alla element x och y och ett fixt heltal n:

$(xy)^n = x^n y^n$, $(xy)^{n+1} = x^{n+1} y^{n+1}$, $(xy)^{n+2} = x^{n+2} y^{n+2}$.

Visa att G är abelsk. Visa också med exempel (t.ex. någon symmetrigrupp) att det inte räcker med att de två första relationerna gäller för något n för att G skall vara abelsk.

GC 5 a) Antag att det existerar en grupp G med generatorer x och y så att $o(x) = 6$, $o(y) = 2$ och $yx = x^5 y$. Visa att i så fall är

$$G = \{x^i y^j;\ i = 0,1,\ldots,5;\ j = 0,1\}.$$

b) Visa att det finns en delgrupp av S_6, som uppfyller villkoren i a).

GC 6 Låt G vara en grupp och H en delgrupp av G. Visa att det finns en 1-1 korrespondens mellan mängden av vänstersidoklasser till H i G och mängden av högersidoklasser till H i G.

GC 7 Låt G vara en grupp.

a) $b \in G$ sägs vara konjugerat till $a \in G$ om det finns $c \in G$ så att $b = c^{-1}ac$. Visa att denna relation är en ekvivalensrelation på G.

b) Den ekvivalensklass som bestäms av a är då mängden $\{c^{-1}ac;\ c \in G\}$. Visa att en ekvivalensklass består av ett enda element om och endast om detta element tillhör centrum av G (se GB 13)

c) Visa att det finns en 1-1 korrespondens mellan den ekvivalensklass som bestäms av a och mängden av högersidoklasser till delgruppen $N_a = \{x \in G;\ ax = xa\}$.
Antalet element i en ekvivalensklass är alltså en delare till G:s ordning.

d) Om speciellt $o(G) = p^n$ (p primtal) och a_m antalet ekvivalensklasser med p^m element (och då a_o = antalet centrumelement), så gäller $p^n = a_o + a_1 p + \ldots + a_{n-1} p^{n-1}$ (det kan inte finnas någon klass med p^n element eftersom e ligger i en klass för sig). Visa nu att centrum till en grupp av ordning p^n måste innehålla andra element än det neutrala elementet.

GC 8 Låt G vara en grupp och M en icke-tom delmängd av G.
Sätt $N(M) = \{a \in G;\ a^{-1} Ma = M\}$, där $a^{-1} Ma = \{a^{-1} xa;\ x \in M\}$ för varje $a \in G$.

a) Visa att N(M) är en delgrupp i G.

b) Visa att index av N(M) i G är lika med antalet olika mängder av formen $a^{-1} Ma$, där $a \in G$.

GC 9 Låt M och N vara normala delgrupper av G sådana att $M \cap N = \{e\}$
Visa att $mn = nm$ för alla $m \in M$, $n \in N$.

GC 10 G är en grupp och H är den minsta delgrupp, som innehåller alla kvadrater g^2, $g \in G$. Visa att H är normal delgrupp i G och att G/H är abelsk.

GC 11 Låt G vara en grupp. Den delgrupp som genereras av alla element av formen $xyx^{-1}y^{-1}$, $x,y \in G$, kallas kommutatordelgruppen.

a) Visa att kommutatordelgruppen är normal i G.

b) Visa att faktorgruppen efter kommutatordelgruppen är abelsk.

c) Visa att om H är normal i G och G/H är abelsk, så är kommutatordelgruppen innehållen i H.

GC 12 En grupp G genereras av två element a och b. N är en normal delgrupp i G. Visa att faktorgruppen G/N är cyklisk om

a) $ab \in N$ b) $aba \in N$ c) $ab^2 \in N$.

GC 13 a) Visa att mängden av transformationer av planet $\mathbb{R}^2$:

$$(x,y) \to (ax + by + r, cx + dy + s) \quad ad - bc \neq 0$$

bildar en grupp G under sammansättning.

b) Visa att mängden N av translationer $(x,y) \to (x+a, y+b)$ bildar en normal delgrupp av G.

c) G/N är isomorf med en annan delgrupp av transformationer. Vilken?

GC 14 En abelsk grupp har 12 element. Visa att man kan finna delgrupper H_1 och H_2 så att $G \supset H_1 \supset H_2 \supset \{e\}$ (äkta inklusion).

GC 15 G är en grupp och M,N normala delgrupper.

a) Visa att $MN = \{mn;\ m \in M,\ n \in N\}$ är en delgrupp av G som omfattar M.

b) Visa att $MN/M \simeq N/(N \cap M)$.

GC 16 Vilka grupper kan vara homomorfa bilder av den cykliska gruppen av ordning p^n (p primtal)?

GC 17 Visa att alla icke-cykliska abelska grupper av ordning p^2 (p primtal) är sinsemellan isomorfa.

GC 18 G är en grupp av udda ordning. Visa att avbildningen $g \to g^2$, $g \in G$, är enentydig. Visa också att avbildningen är en automorfism om och endast om G är en abelsk grupp.

GC 19 Konstruera en injektiv grupphomomorfism $S_n \to A_{n+2}$.

GC 20 Låt P beteckna mängden av alla n x n-matriser bestående av endast nollor och ettor, sådana att varje rad och varje kolonn innehåller precis en etta.

a) Visa att P är en delgrupp av den multiplikativa gruppen av invertibla n x n-matriser (med reella koefficienter).

b) Visa att gruppen P är isomorf med den symmetriska gruppen S_n.

Svar

GA 1 a) (ii) b) (i), (ii), (iii) 0, (iv) alla element utom 1
c) - d) (i), (ii), e) (i), (ii), (iii) 0, (iv) bara 0
f) (i), (ii), (iii) $\emptyset$, (iv) bara $\emptyset$ g) (i) h) (iii) 1,
(iv) varje element är sin egen invers

GA 2 a), b), e), g), i), k), l), m)

GA 3 b)

GA 4 $ab = ba = c$, $ac = ca = b$, $bc = cb = a$.

GA 5 b) $\varepsilon = (0,0)$; till $\alpha = (a,b)$, ta $\beta = (-a,-a)$ c) nej

GA 9 a) $x = a^{-1}bca^{-1}b^{-1}a^{-1}$ b) $x = b^{-1}a$ c) $x = a^{-3}$

GA 10 $\{\overline{0}\}$, $\{\overline{0},\overline{9}\}$, $\{\overline{0},\overline{6},\overline{12}\}$, $\{\overline{0},\overline{3},\overline{6},\overline{9},\overline{12},\overline{15}\}$, $\{\overline{0},\overline{2},\overline{4},\overline{6},\overline{8},\overline{10},\overline{12},\overline{14},\overline{16}\}$, $\mathbb{Z}_{18}$

GA 11 $\{\overline{0},\overline{4},\overline{8}\}$, $\{\overline{0},\overline{2},\overline{4},\overline{6},\overline{8},\overline{10}\}$, $\mathbb{Z}_{12}$

GA 12 T.ex. $\{n\pi \mid n \in \mathbb{Z}\}$

GA 13 Ja.

GA 15 Av ordning 1 : $\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$, av ordning 2: $\begin{pmatrix}1 & 0\\ 1 & -1\end{pmatrix}$, $\begin{pmatrix}0 & -1\\ -1 & 0\end{pmatrix}$, $\begin{pmatrix}-1 & 1\\ 0 & 1\end{pmatrix}$,
av ordning 3: $\begin{pmatrix}-1 & 1\\ -1 & 0\end{pmatrix}$, $\begin{pmatrix}0 & -1\\ 1 & -1\end{pmatrix}$.

GA 16 $o(\overline{1}) = \overline{1}$, $o(\overline{2}) = o(\overline{4}) = 3$, $o(\overline{6}) = 2$, $o(\overline{3}) = o(\overline{5}) = 6$. Ja.

GA 17 b) 12 c) Ja ; genererad av t.ex. $(\overline{1},\overline{1})$.

GA 18 a) $\{I\}$, $\{I,R_2\}$, $\{I,V\}$, $\{I,H\}$, $\{I,D_1\}$, $\{I,D_2\}$, $\{I,R_1,R_2,R_3\}$,
$\{I,V,H,R_2\}$, $\{I,D_1,D_2,R_2\}$, hela gruppen.
b) de 7 första i svaret på a).
c) $\{I,V,H,R_2\}$ resp. hela gruppen

d) för $\{I,V\}$ vänster: $\{I,V\}$, $\{R_1,D_1\}$, $\{R_2,H\}$, $\{R_3,D_2\}$

höger: $\{I,V\}$, $\{R_1,D_2\}$, $\{R_2,H\}$, $\{R_3,D_1\}$

för $\{I,R_2\}$ vänster: $\{I,R_2\}$, $\{R_1,R_3\}$, $\{V,H\}$, $\{D_1,D_2\}$

höger: $\{I,R_2\}$, $\{R_1,R_3\}$, $\{V,H\}$, $\{D_1,D_2\}$

för $\{I,V,H,R_2\}$ vänster: $\{I,V,H,R_2\}$, $\{R_1,D_1,D_2,R_3\}$

höger: $\{I,V,H,R_2\}$, $\{R_1,D_1,D_2,R_3\}$.

e) $\{I,R_2\}$ och $\{I,V,H,R_2\}$.

f)

	$\{I,R_2\}$	$\{R_1,R_3\}$	$\{V,H\}$	$\{D_1,D_2\}$
$\{I,R_2\}$	$\{I,R_2\}$	$\{R_1,R_3\}$	$\{V,H\}$	$\{D_1,D_2\}$
$\{R_1,R_3\}$	$\{R_1,R_3\}$	$\{I,R_2\}$	$\{D_1,D_2\}$	$\{V,H\}$
$\{V,H\}$	$\{V,H\}$	$\{D_1,D_2\}$	$\{I,R_2\}$	$\{R_1,R_3\}$
$\{D_1,D_2\}$	$\{D_1,D_2\}$	$\{V,H\}$	$\{R_1,R_3\}$	$\{I,R_2\}$

GA 19

	$\{\bar{1},\bar{4}\}$	$\{\bar{2},\bar{8}\}$	$\{\bar{7},\overline{13}\}$	$\{\overline{11},\overline{14}\}$
$\{\bar{1},\bar{4}\}$	$\{\bar{1},\bar{4}\}$	$\{\bar{2},\bar{8}\}$	$\{\bar{7},\overline{13}\}$	$\{\overline{11},\overline{14}\}$
$\{\bar{2},\bar{8}\}$	$\{\bar{2},\bar{8}\}$	$\{\bar{1},\bar{4}\}$	$\{\overline{11},\overline{14}\}$	$\{\bar{7},\overline{13}\}$
$\{\bar{7},\overline{13}\}$	$\{\bar{7},\overline{13}\}$	$\{\overline{11},\overline{14}\}$	$\{\bar{1},\bar{4}\}$	$\{\bar{2},\bar{8}\}$
$\{\overline{11},\overline{14}\}$	$\{\overline{11},\overline{14}\}$	$\{\bar{7},\overline{13}\}$	$\{\bar{2},\bar{8}\}$	$\{\bar{1},\bar{4}\}$

GA 23 d) $\mathbb{N}$ e) $(\mathbb{R}\setminus\{0\},.)$

GA 24 b) $\operatorname{Ker}\phi = \{0\}$ c) $\operatorname{Ker}\phi = \{+1\}$, e) $\operatorname{Ker}\phi = \{0\}$,

g) $\operatorname{Ker}\phi = \{\bar{0},\bar{3},\bar{6},\bar{9},\overline{12},\overline{15} \bmod 18\}$,

h) $\operatorname{Ker}\phi = \{A \in G \mid \det A = 1\}$ i) $\operatorname{Ker}\phi = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{R} \right\}$.

GA 25 a) $\mathbb{Z}_8 \ni \bar{a} \to \bar{a} \in \mathbb{Z}_4$ el. $\mathbb{Z}_8 \ni \bar{a} \to \overline{2a} \in \mathbb{Z}_4$ el. $\mathbb{Z}_8 \ni \bar{a} \to \overline{3a} \in \mathbb{Z}_4$

b) finns ingen

GA 26 f är en homomorfism om och endast om G är abelsk. Då är f också en automorfism.

GA 27 $G_1 \simeq G_3$, $G_2 \simeq G_4$, men $G_1 \not\simeq G_2$.

GA 28 $\overline{1} \to \overline{\overline{3}}$, $\overline{2} \to \overline{\overline{2}}$, $\overline{3} \to \overline{\overline{6}}$, $\overline{4} \to \overline{\overline{4}}$, $\overline{5} \to \overline{\overline{5}}$, $\overline{0} \to \overline{\overline{1}}$ (ett streck är restklass modulo 6, två streck är restklass modulo 7)

GA 30 Ta ϕ: $\mathbb{C} \to \mathbb{R}$ så att $\phi(z) = \mathrm{Re}\ z$

GA 31 d) två automorfier av $\mathbf{Z}_6$: den identiska avbildningen och avbildningen $\overline{a} \to -\overline{a}$.

GA 33 b) {0} och den cykliska gruppen av ordning 17 resp.
{0} och de cykliska grupperna av ordning 2,3,6,9,18.

GA 34 Kärnan = $4\mathbb{Z} = \{4n \mid n \in \mathbb{Z}\}$.

GA 35 a) (1,2)(3,6,5,4) b) (1,3,4,5,6)(2,7) c) (1,7)(2,3,4,5,6)
d) (1,6,3,4,7)(2,5) e) (1,4,7,3,2)(5,6) f) (1,2,3,4,5,6,7)

GA 36 (1,3,5,7,9,11)(2,4,6,8,10,12), (1,4,7,10)(2,5,8,11)(3,6,9,12), (1,5,9)(2,6,10)(3,7,11)(4,8,12), (1,6,11,4,9,2,7,12,5,10,3,8), (1,7)(2,8)(3,9)(4,10)(5,11)(6,12).

GA 37 b) (1,2)(3,4,5,6), (1,6,5,4,3)(2,7), (1,7)(6,5,4,3,2), (1,7,4,3,6)(2,5); (1,2,3,7,4)(5,6), (1,7,6,5,4,3,2)

GA 38 b) m udda c) permutationerna i b),c),d),e)

GA 39 b) $(1)V = \{(1),(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\} = V(1)$
$(1,2)V = \{(1,2),(3,4),(1,4,2,3),(1,3,2,4)\} = V(1,2)$
$(1,3)V = \{(1,3),(1,4,3,2),(2,4),(1,2,3,4)\} = V(1,3)$
$(2,3)V = \{(2,3),(1,2,4,3),(1,3,4,2),(1,4)\} = V(2,3)$
$(1,2,3)V = \{(1,2,3),(2,4,3),(1,4,2),(1,3,4)\} = V(1,2,3)$
$(1,3,2)V = \{(1,3,2),(1,4,3),(2,3,4),(1,2,4)\} = V(1,3,2)$
V är alltså normal i S_4.
c) En homomorfism $S_3 \to S_4/V$ ges av att $\phi \in S_3$ avbildas på $\phi V \in S_4/V$.

GB 1 $\{id, f, g, 1-x, \frac{x}{x-1}, \frac{x-1}{x}\}$.

GB 2 b) $\phi(n)$ (se uppgift I 21)

c) $\{\overline{1}, \overline{5}, \overline{7}, \overline{11}, \overline{13}, \overline{17}\}$. Ja, genererad av $\overline{5}$ t.ex.

d) $\{\overline{1}, \overline{2}, \overline{4}, \overline{8}\}$ eller $\{\overline{1}, \overline{7}, \overline{4}, \overline{13}\}$ modulo 15.

GB 3 b) $\{\pm 1\}$ c) $\{z \in \mathbb{C} \mid z^n = 1$ för något $n \in \mathbb{Z}_+\}$.

GB 13 b) hela gruppen c) $\{e\}$ d) $\{I, R_2\}$.

GB 15 a) $\{E, A, A^2, A^3, B, B^3, AB, BA\}$, där E är enhetsmatrisen.

b) $o(A) = o(A^3) = o(B) = o(B^3) = o(AB) = o(BA) = 4$, $o(A^2) = 2$.

c) $\{E\}$, $\{E, A^2\}$, $\{E, A, A^2, A^3\}$, $\{E, B, A^2, B^3\}$, $\{E, AB, A^2, BA\}$.

GB 18 T.ex. $G = S_3$, N = delgruppen genererad av ett av elementen av ordning 3. Då är G/N av ordning 2, alltså abelsk.

GB 19 Kärnan är $\{(4t, -t, -3t) \in \mathbb{R}^3 \mid t \in \mathbb{R}\}$.

GB 24 b) $o(f(x)) \mid o(x)$.

GB 25 e och x^{29}, där x är G:s generator.

GB 26 $\mathbb{Z}_{15}^* = \{\overline{1}, \overline{2}, \overline{4}, \overline{7}, \overline{8}, \overline{11}, \overline{13}, \overline{14}\}$ resp. $Z_{24}^* = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}, \overline{13}, \overline{17}, \overline{19}, \overline{23}\}$; de är inte isomorfa.

GB 29 Varje automorfism är bestämd av bilderna av a och b. Det finns 6 automorfismer: id, $\begin{cases} a \to a \\ b \to ab \end{cases}$, $\begin{cases} a \to b \\ b \to a \end{cases}$, $\begin{cases} a \to b \\ b \to ab \end{cases}$, $\begin{cases} a \to ab \\ b \to b \end{cases}$, $\begin{cases} a \to ab \\ b \to a \end{cases}$,

som bildar en grupp isomorf med S_3.

GB 31 Ja; varje avbildning som permuterar a,b,c på ett fixt sätt är en automorfism.

GB 32 id, $\begin{cases} a \to a \\ b \to ab \end{cases}$ inre, $\begin{cases} a \to a \\ b \to a^2b \end{cases}$ inre, $\begin{cases} a \to a \\ b \to a^3b \end{cases}$, $\begin{cases} a \to a^3 \\ b \to b \end{cases}$ inre, $\begin{cases} a \to a^3 \\ b \to ab \end{cases}$, $\begin{cases} a \to a^3 \\ b \to a^2b \end{cases}$ inre, $\begin{cases} a \to a^3 \\ b \to a^3b \end{cases}$

GB 33 a) k b) minsta gemensamma multipeln till $m_1, m_2, \ldots, m_k$.

GB 34 144 resp. 80

GB 35 a) (2,3,5,4),(1,3,2,5,4),(1,5,4,3).

b) aba^2, a^3ba, a^2ba^3.

GB 36 a) T.ex. $G = S_4$, $a = (1,2)$, $b = (1,3,4)$

b) 12

GB 38 a) (1,2)(3,4,5)(6,7,8,9,10) resp. (3,4)(6,7,8,9,10).

b) H genereras av (1,2),(3,4),(3,4,5) och (6,7,8,9,10).

c) 60

GB 39 b) t.ex. $a = (1,2)(4,5,6)$.

GB 40 a) $(a_1, a_2, \ldots, a_5)$ där $a_i \in \{1,2,3,4,5\}$ och $a_i \neq a_j$ om $i \neq j$.

GC 1 Den cykliska gruppen och $\{e,a,b,ab \mid a^2 = b^2 = e,\ ab = ba\}$.

GC 2 Den cykliska gruppen och S_3.

GC 3 Den cykliska gruppen och $\{e,a,a^2,a^3,a^4,b,ab,a^2b,a^3b,a^4b \mid a^5 = b^2 = e,\ ba = a^4b\}$.

GC 4 Ta S_3 och $n = 6$.

GC 5 b) T.ex. den delgrupp, som genereras av (1,2,3,4,5,6) och (2,6)(3,5).

GC 13 c) $\{(x,y) \to (ax + by,\ cx + dy)\}$.

GC 16 De cykliska grupperna av ordning p^k, där $0 \leq k \leq n$.

GC 19 $\begin{cases} \tau \to \tau & \text{, om } \tau \in S_n \text{ jämn} \\ \tau \to \tau\,(n+1,n+2) & \text{, om } \tau \in S_n \text{ udda} \end{cases}$

Ledningar

GA 1 (i) Associativitet framgår inte direkt ur kompositionstabell utan måste prövas. När $a * b$ ges genom en formel, jämför $(a * b) * c$ och $a * (b * c)$.

(ii) Kommutativitet syns direkt ur en tabell: elementet på plats (i,j) = elementet på plats (j,i) dvs tabellen är symmetrisk kring huvuddiagonalen. När $a * b$ ges genom en formel, jämför $a * b$ och $b * a$.

(iii) Existens av neutralt element syns direkt i tabell: dess rad och kolonn är identiska med överraden resp. ytterkolonnen. När $a * b$ ges genom en formel, så satisfierar neutrala elementet ekvationen $a * x = x * a = a$ för alla a.

(iv) Invers till element syns direkt i tabell: a:s invers är det element i överraden som ger det neutrala elementet i a:s rad. Kontrollera att samma element i ytterkolonnen ger det neutrala elementet i a:s kolonn. Om $a * b$ ges genom en formel, lös ekvationen $a * y = y * a =$ det neutrala elementet.

GA 2 Se GA 1. Om M är ändlig, gör kompositionstabell och avläs villkoren som i GA 1. Addition och multiplikation av tal, restklasser, matriser är säkert associativa liksom funktionssammansättning.

GA 3 $x * g = y * g \Rightarrow x = y$ för element i en grupp. I en gruppbell innehåller därför varje kolonn varje gruppelement precis en gång.

GA 4 se GA 3.

GA 5 Lös $\alpha * x = \alpha$ för att få $x = \varepsilon$ och sedan $y * \alpha = \varepsilon$.

GA 7 Visa att $(a^{-1}ba)^k = a^{-1}b^k a$.

GA 8 Skriv högerledet utan exponent och multiplicera likheten med lämpliga element till vänster resp. till höger.

GA 9 b) multiplicera den första ekvationen med x.
c) $x^9 = x^{-1}$ fås ur $x^5 = e$. Bestäm också x^9 ur den andra ekvationen.

GA 15 Ett elements ordning bestäms genom uträkning av potenserna i tur och ordning. Enligt Lagranges sats kan man begränsa sig till att pröva de potenser x^k för vilka $k \mid o(G)$.

GA 16 En grupp är cyklisk om och endast om den har ett element av samma ordning som gruppen.

GA 17 c) Finns element med samma ordning som gruppen?

GA 20 Använd det (AB) = detA·detB.
Visa att alla element A,B som inte ligger i H är kongruenta modulo H, dvs $AB^{-1} \in H$.

GA 22 En av sidoklasserna är delgruppen själv och de två klasserna tillsammans fyller upp gruppen.

GA 25 Visa att varje homomorfism av $\mathbf{Z}_8$ är bestämd av $\bar{1}$:s bild, och undersök sedan på vilka element i $\mathbf{Z}_4$ resp. $\mathbf{Z}_5$ det är möjligt att avbilda $\bar{1}$ ($\bar{1}$ avbildas inte på $\bar{0}$ eftersom homomorfismen skall vara $\neq 0$).

GA 28 $\bar{2} = \bar{1} + \bar{1}$, $\bar{3} = \bar{1} + \bar{1} + \bar{1}$ osv i $\mathbf{Z}_6$ medför att bilderna av elementen i $\mathbf{Z}_6$ är bestämda av bilden av $\bar{1}$.

GA 31 a) jfr GA 28 c) Gör kompositionstabell
d) p.s.s. som i a) inses att en homomorfism $\mathbf{Z}_6 \to \mathbf{Z}_6$ är bestämd av bilden av $\bar{1}$. Varför är avbildningen som tar $\bar{1}$ till $\bar{2}$ inte en automorfism?

GA 32 a) Använd att $n = 1 + 1 + \ldots + 1$ (n st) och $1 = 1/n + 1/n + \ldots + 1/n$ (n st) om $n > 0$, samt att $\phi(x) = -\phi(-x)$ om $x < 0$.

GA 33 a) Visa att bilden av generatorn är en generator i den homomorfa bilden.

GA 34 Visa att den ändliga gruppen är cyklisk och låt dess generator vara bild av generatorn i $(\mathbf{Z},+)$.

GA 37 a) Multiplicera $(a_1,a_2,\ldots,a_n)$ med $(a_n,\ldots,a_2,a_1)$.

b) Använd a) och att $(xy)^{-1} = y^{-1}x^{-1}$

GB 1 Börja konstruera en kompositionstabell genom att sätta e,f,g i överraden och ytterkolumnen och skriv in motsvarande produkter. Varje gång man får ett nytt element som produkt förs det in i överraden och ytterkolumnen, och multiplikationen går vidare.

GB 3 a) Visa att $o(ab) \leq o(a)o(b)$.

b) Visa att produkten av $\begin{pmatrix} 1 & a \\ 0 & -1 \end{pmatrix}$ och $\begin{pmatrix} 1 & b \\ 0 & -1 \end{pmatrix}$ för $a \neq b$ inte har ändlig ordning.

GB 4 a) Visa att $(ba)^{-1} = (ab)^{-1}$ b) Lös ut b

c) Visa att $(ab =) b^{-2}a^{-1} = b^{-1}a^{-1}b^{-1}$.

För det sista påståendet, betrakta den minsta icke-abelska gruppen, dvs S_3.

GB 5 a) Använd att $(ab)^{-1} = b^{-1}a^{-1}$ och att varje element är sin egen invers.

b) Visa att om $a_1,\ldots,a_k$ är en minimal mängd generatorer för G, så är $G = \{a_1^{i_1} \cdot \ldots \cdot a_k^{i_k} ; i_j = 0,1 \text{ och } j = 1,\ldots,k\}$.

GB 6 Skriv $m = qo(a) + r$, där $0 \leq r < o(a)$ och använd att $o(a)$ är det minsta heltal n så att $a^n = e$.

GB 7 x^k är generator om och endast om $o(x^k) = o(a)$. Vad är $o(x^r)$ om $o(a) = rs$?

GB 8 b) Visa att om $(ab)^n = e$, så är också $(ba)^n = e$ genom att utveckla potensen $(ab)^n$ och multiplicera den förra likheten med lämpliga element till vänster resp. till höger. Använd också GB 6. Visa sedan med hjälp av det föregående att $o(ab) = \infty$ om och endast om $o(ba) = \infty$.

GB 9 Visa att relationen $x \sim y \Leftrightarrow (x = y$ eller $x = y^{-1})$ är en ekvivalensrelation på G. x:s ekvivalensklass innehåller ett element om $x = x^{-1}$, och två element om $x \neq x^{-1}$.

GB 10 Visa att $xax^{-1} = a$ för alla $x \in G$, genom att undersöka $o(xax^{-1})$.

GB 11 Om $G = (x)$, och $H \leqq G$, så låt k vara det minsta pos. heltal sådant att $x^k \in H$. Visa att $H = (x^k)$ genom att för $x^m \in H$ skriva $m = qk + r$, där $0 \leq r < k$.

GB 12 Ta $x \in H \cap K$ och använd Lagranges sats för att visa att $o(a) = 1$.

GB 14 a) Visa att avbildningen $H \to gHg^{-1}$, som tar h till ghg^{-1} ger en 1-1 korrespondens mellan H och gHg^{-1}.

b) Använd a).

GB 15 d) Använd övningarna GA 22 och GB 14 b).

GB 16 Vad är $(Na)^{o(a)}$?

GB 17 Använd Lagranges sats och GB 16 för att visa att $o(Na) = 1$.

GB 21 Tänk på att $a^{x+y} = a^x a^y$.

GB 22 Avbilda generator på generator. Tänk på att Du måste visa att avbildningen är väldefinierad: $x^k = x^l \Rightarrow (x^k) = (x^l)$.
Men $x^k = x^l$ om och endast om $o(G) | (k-1)$.

GB 23 Tänk på att neutralt element avbildas på neutralt element och försök med hjälp av detta att konstruera en isomorfism.

GB 25 Använd GB 24 a).

GB 26 Undersök elementens ordningar och använd GB 24 a).

GB 27 b) Betrakta $\mathbb{C} \setminus \{0\} \to \mathbb{R}_+$ given av att $z \to |z|$.

GB 28 $T = \{e^{ir};\ r \in \mathbb{R}\}$. Försök konstruera en homomorfism av $\mathbb{R}$ på T med $\mathbb{Z}$ som kärna ($e^{2\pi in} = 1$ för $n \in \mathbb{Z}$).

GB 29 G genereras av a och b, alltså är varje automorfism bestämd av bilderna av a och b. Hur kan dessa väljas?

GB 30 a) Visa att $x \to a^{-1}xa$ är olika för olika $a \in S_3$.

b) S_3 genereras av ett element av ordning 2 och ett element av ordning 3. Använd GB 24 a) för att undersöka hur de kan avbildas av en automorfism.

GB 32 G genereras av a och b. Använd GB 24 a) för att undersöka vilka element a och b kan avbildas på. Varför kan b inte avbildas på a^2? Visa att avbildningarna $x \to c^{-1}xc$ är parvis lika när c genomlöper G, genom att bestämma a:s och b:s bilder.

GB 33 b) Låt $\tau_1,\ldots,\tau_k$ vara disjunkta cykler i S_n och visa att $(\tau_1\tau_2\ldots\tau_k)^s = \tau_1^s\,\tau_2^s\ldots\tau_k^s = e$ om och endast om varje $\tau_i^s = e$.

GB 34 Elementen av ordning 3 är dels 3-cyklerna, dels produkterna av två disjunkta 3-cykler. Varje mängd av k tal ger (k-1)! olika k-cykler.

GB 35 b) $b^2 = e$. bab, ba^2b, ba^3b löses ur likheten i a).

c) ett godtyckligt element i H av formen $a^{i_1}ba^{i_2}b\ldots ba^{i_k}$ skrivs om med hjälp av b).

GB 36 a) Betrakta en symmetrisk grupp.

b) $o(ab)^{12} = e$ klart. Kan någon lägre potens vara = e?

GB 37 b) Visa att H_a är isomorf med A_{n-1} för a = 1,2,...,n.

GB 38 c) Sätt $a = \rho^{15}$, $b = \rho^{10}$, $c = \rho^6$, $d = \tau^5$. Då är $H = \{a^i b^{j_1} d^{k_1} b^{j_2}\ldots b^{j_n} d^{k_n} c^l$; $i = 0,1$, $j_t = 0,1,2, k_t = 0,1$, $l = 0,1,\ldots,4\}$. Hur många element av formen $b^{j_1} d^{k_1}\ldots b^{j_n} d^{k_n}$ finns det?

GB 39 b) $a^{-1}x_1x_2a = a^{-1}x_1a \cdot a^{-1}x_2a$.

c) Undersök om de båda leden har samma paritet (dvs om de är båda udda eller båda jämna).

GB 40 a) jfr GB 33

b) om $H = ((a_1,a_2,\ldots,a_5))$, undersök $(a_1,a_2)H(a_1,a_2)$; Du kan också använda GB 39 d).

c) Använd homomorfisatsen.

GC 1 Om gruppen inte är cyklisk, är alla element av ordning 2. Hur ser då kompositionstabellen ut?

GC 2 Antag att gruppen inte är cyklisk. Den har då ett element a av ordning 2 (GB 9) och ett element b av ordning 3 (GB 5), $ab \neq ba$ (varför?). Gör kompositionstabell.

GC 3 Antag att gruppen inte är cyklisk. Den har då ett element a av ordning 2 och ett element b av ordning 5, $ab \neq ba$ (jfr GC 2). Visa att $ba \neq ab^2, ab^3$ genom att härleda motsägelser ur likheterna $ba = ab^2$ resp. $ba = ab^3$. Gör kompositionstabell. Kontrollera associativiteten genom att jämföra med en delgrupp av S_5.

GC 4 Multiplicera den första likheten med xy och jämför med den andra likheten; gör motsvarande med andra och tredje likheterna. Tänk på att för $n = o(G)$ är $x^n = e$ och $x^{n+1} = x$.

GC 5 b) Betrakta en regelbunden sexhörning; låt x vara en rotation 1/6 varv och y en spegling. Numrera hörnen och gå över till S_6.

GC 6 Avbildningen som tar Ha till aH är inte väldefinierad (varför?). Pröva den som tar Ha till $a^{-1}H$.

GC 7 c) Visa att avbildningen som tar $c^{-1}ac$ i ekvivalensklassen till sidoklassen $N_a c$ är väldefinierad (dvs $c^{-1}ac = d^{-1}ad \Rightarrow N_a c = N_a d$) och ger 1-1 korrespondensen.

d) Dividera båda leden i likheten med p.

GC 8 b) Visa att avbildningen $N(M)a \to a^{-1}N\,a$ är väldefinierad och ger en 1-1 korrespondens mellan mängden av sidoklasser till N(M) och mängden av mängder av formen $a^{-1}M\,a$.

GC 9 Visa att $mnm^{-1}n^{-1} \in M \cap N$.

GC 10 $h^{-1}g^2h = (h^{-1}gh)^2$. För det andra påståendet, använd GB 5.

GC 11 a) $g^{-1}xyx^{-1}y^{-1}g = g^{-1}xg \cdot g^{-1}yg \cdot (g^{-1}xg)^{-1} \cdot (g^{-1}yg)^{-1}$.

b), c) $\bar{G}$ är abelsk om och endast om $a\,b\,a^{-1}b^{-1} = e$ för alla $a,b \in \bar{G}$.

GC 12 Faktorgruppen genereras då av Na och Nb; de olika villkoren på a,b innebär att Na är en potens av Nb (eller tvärtom).

GC 13 c) Elementen i N är precis de som har matrisen $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

GC 14 Det finns en delgrupp H_2 av ordning 2 enligt GB 9. Finn H_1 genom att betrakta G/H_2.

GC 15 b) Betrakta avbildningen $N \to MN/M$ som tar n till Mn.

GC 16 Använd GA 33 och GB 22.

GC 17 Visa att det finns två element x och y av ordning p, så att $(x) \cap (y) = \{e\}$, och hela gruppen genereras av x och y.

GC 18 $o(G) = 2n + 1$ medför att $x^{2n+1} = e$; härled enentydigheten ur detta. Se vidare I 4 och GA 8.

GC 19 För att bilden av en udda permutation skall bli jämn, lägg till en transposition: (n+1,n+2).

GC 20 a) Det räcker att kontrollera slutenheten, som följer direkt ur definitionen av matrismultiplikation.

b) Till varje matris i P ordnas en permutation i S_n: den permutation som tar i till radindex för 1:an i i:te kolonnen. Omvänt ger detta en avbildning från S_n till P.

Lösningar

GA 1 a) Prövning av olika kombinationer av tre element ger att t.ex. $a_2 * (a_3 * a_4) = a_1 \neq a_3 = (a_2 * a_3) * a_4$. $*$ är alltså inte associativ.

är kommutativ om och endast om elementet i rad i och kolonn j är lika med elementet i rad j och kolonn i, dvs om och endast om tabellen är symmetrisk kring huvuddiagonalen. Alltså är kommutativ i detta fall.

Inspektion av tabellen visar att det inte finns ngt $x \in M$ så att $x * a_i = a_i$ för alla $a_i \in M$. Neutralt element saknas alltså.

b) $(a * b) * c = (a + b - ab) * c = a + b - ab + c - ac - bc + abc$ och $a * (b * c) = a * (b + c - bc) = a + b + c - bc - ab - ac + abc$, varav följer att $*$ är associativ. Klart att $a * b = b * a$, så att $*$ är kommutativ.

Ett ev. neutralt element x satisfierar ekvationen $a * x = a + x - ax = a$ för alla $a \in M$. Man får $x(1 - a) = 0$ för alla $a \in M$, dvs $x = 0$.

För en ev. invers y till $a \in M$ gäller $a * y = a + y - ay = 0$, dvs $y(1 - a) = -a$. Ekvationen har lösningen $y = a/(1 - a)$ om $a \neq 1$ och saknar lösning för $a = 1$.

c) - f) jfr b)

g) - h) jfr a).

GA 2 b) $a/b * c/d = (ad + bc)/bd \in M$, ty produkten av två udda tal är udda.

Addition av rationella tal är associativ.

$0 = 0/1 \in M$ är neutralt element. Till $a/b \in M$ är $-a/b \in M$ invers.

$(M, *)$ är alltså en grupp.

c) $a/b * c/d = (ac)/(bd) \in M$, ty $ac \neq 0$ om $a \neq 0$, $c \neq 0$ och bd udda om b,d udda.

Multiplikation av rationella tal är associativ.

$1 = 1/1 \notin M$ är neutralt element. Alla tal i M med jämn täljare saknar invers. Alltså är M inte en grupp under $*$.

g) Gör en kompositionstabell:

$*$	$\overline{1}$	$\overline{5}$	$\overline{7}$	$\overline{11}$
$\overline{1}$	$\overline{1}$	$\overline{5}$	$\overline{7}$	$\overline{11}$
$\overline{5}$	$\overline{5}$	$\overline{1}$	$\overline{11}$	$\overline{7}$
$\overline{7}$	$\overline{7}$	$\overline{11}$	$\overline{1}$	$\overline{5}$
$\overline{11}$	$\overline{11}$	$\overline{7}$	$\overline{5}$	$\overline{1}$

Av tabellen framgår att M är sluten under $*$. Vidare är restklassmultiplikation associativ. $\overline{1}$ är neutralt element, och av tabellen syns att varje element är sin egen invers.

h), i) och l) görs i analogi med g).

GA 3 a) Vi ser att $a * b = d * b = b$. Men i en grupp måste enligt annuleringslagarna gälla att $g * x = h * x \Rightarrow g = h$. Tabellen representerar inte en grupp.

b) $\{a,b,c,d\}$ är sluten under kompositionen, c är neutralt element och varje element är sin egen invers. Återstår att undersöka associativiteten. Vi skall jämföra $(x * y) * z$ och $x * (y * z)$ för $x,y,z \in \{a,b,c,d\}$. Totalt finns 64 olika kombinationer att undersöka och även om man för många av dessa direkt kan säga att det associativa villkoret gäller, så blir kontrollen tidsödande och tråkig. Men om vi kan finna en konkret mängd M med 4 element och en associativ komposition $*$ sådan att om vi identifierar a,b,c,d med M:s element så ger tabellen kompositionstabellen för $*$ i M, så måste tabellen representera en associativ komposition. GA 2 g) ger lämpliga M och $*$.

GA 4 Tabellen kan bara fullbordas på ett enda sätt så att annulleringslagarna gäller. För associativiteten se GA 3 b).

GA 5 b) För $\alpha = (a,b)$ lös ekvationen $(a,b) * (x_1,x_2) = (a,b)$. Vi får $x_2 = 0$. Varje element $(c,0)$ är alltså högerneutralt. Lös $(y_1,y_2) * (a,b) = (c,0)$. Vi får $y_1 = c - a, y_2 = -a$.

c) $(c,0) * (a,b) = (c+a,a) \neq (a,b)$ om $b \neq a$. Inget element är alltså neutralt element.

GA 8 Vi har $aabb = abab$. Multiplicera t.v. med a^{-1} och t.h. med b^{-1}. Vi får $(a^{-1}a)ab(bb^{-1}) = (a^{-1}a)ba(bb^{-1})$, dvs $ab = ba$.

GA 9 a) Multiplikation t.v. med x^{-1} ger $axaba = bc$. Multiplikation t.v med a^{-1} och t.h. med $(aba)^{-1}$ ger $x = a^{-1}bc(aba)^{-1}$.

b) Vi får $ax^3 = bx$, dvs $a = bx$, så att $x = b^{-1}a$.

c) $x^{10} = e \Rightarrow x^9 = x^{-1}$. Men $x^9 = a^3$. Alltså $x = a^{-3}$.

GA 14 $x,y \in N_a \Rightarrow a(xy) = (ax)y = (xa)y = x(ay) = x(ya) = (xy)a \Rightarrow xy \in N_a$.
$x \in N_a \Rightarrow ax = xa \Rightarrow x^{-1}axx^{-1} = x^{-1}xax^{-1} \Rightarrow x^{-1}a = ax^{-1} \Rightarrow x^{-1} \in N_a$.

GA 16 Gruppegenskapen visas med kompositionstabell som i GA 2 g).
För att bestämma ordningen av $\overline{2}$ undersöker vi potenserna av $\overline{2}$:
$\overline{2}^2 = \overline{4} \neq \overline{1}$, $\overline{2}^3 = \overline{1} \Rightarrow o(\overline{2}) = 3$. De övriga elementens ordningar bestäms analogt. Vi ser att $o(\overline{3}) = 6$ = gruppens ordning. Den delgrupp som genereras av $\overline{3}$ är alltså hela gruppen, dvs gruppen är cyklisk.

GA 20 $A,B \in H \Rightarrow \det(A) > 0, \det(B) > 0 \Rightarrow \det(AB) = \det(A) \cdot \det(B) > 0 \Rightarrow AB \in H$
$A \in H \Rightarrow \det(A) > 0 \Rightarrow \det(A^{-1}) = 1/\det(A) > 0 \Rightarrow A^{-1} \in H$. H är alltså en delgrupp.
Ta $C,D \notin H$, dvs $\det(C) < 0$, $\det(D) < 0$. Då är $\det(CD^{-1}) > 0$, så $CD^{-1} \in H$. Det betyder att alla element som inte ligger i H är kongruenta modulo H. Alltså finns bara två sidoklasser till H; H själv och komplementet till H.

GA 21 Att mängden är en delgrupp visas på samma sätt som i GA 20.

För att visa att den är normal, ta A med det(A) = 1 och inverterbar 2 x 2-matris B. $\det(BAB^{-1}) = \det(B) \cdot 1 \cdot \det(B^{-1}) = \det(BB^{-1}) = 1$, så att $BAB^{-1} \in$ delgruppen.

GA 22 Låt G vara en grupp och H en delgrupp av index 2. Om $a \in G \setminus H$, så är $G = H \cup Ha$, eftersom det bara finns två sidoklasser. Analogt är $G = H \cup aH$, dvs $G \setminus H = Ha = aH$.

GA 23 a) Gruppaxiomen verifieras genom explicita räkningar.

Man får att $(a,b)^{-1} = (-a/b, 1/b)$.

b) $(a,1) * (b,1) = (a+b,1)$ och $(a,1)^{-1} = (-a,1)$ ger att N är en delgrupp. Vidare är $(c,d) * (a,1) * (c,d)^{-1} = (ad,1) \in N$, så N normal.

c) $\phi((a,b) * (c,d)) = \phi((a+bc,bd)) = bd = \phi((a,b)) \cdot \phi((c,d))$.

d) Ker $\phi = \{(a,b) \in G;\ \phi((a,b)) =$ det neutrala elementet i $\mathbb{R} \setminus \{0\} = 1\} = N$.

e) ϕ är på, så homomorfisatsen ger $G/N \simeq \mathbb{R} \setminus \{0\}$.

GA 24 f) $\phi(\frac{1}{2} + \frac{1}{2}) = \phi(1) = 1$ men $\phi(\frac{1}{2}) + \phi(\frac{1}{2}) = 0 + 0 = 0$.

ϕ är alltså inte en homomorfism.

GA 25 a) om ϕ är en homomorfism från $\mathbb{Z}_8$ till $\mathbb{Z}_4$ så är $\phi(\bar{a}) = a\phi(\bar{1})$, ty $\bar{a} = \bar{1} + \bar{1} + \ldots + \bar{1}$ (a st), vilket ger $\phi(\bar{a}) = \phi(\bar{1}) + \ldots + \phi(\bar{1})$ (a st). På vilket element i $\mathbb{Z}_4$ kan $\bar{1} \in \mathbb{Z}_8$ avbildas? Inte på $\bar{0}$, ty då blir homomorfismen 0. $\bar{1}$ är möjlig. Då får man $\phi(\bar{0}) = \phi(\bar{4}) = \bar{0}$, $\phi(\bar{1}) = \phi(\bar{5}) = \bar{1}$, $\phi(\bar{2}) = \phi(\bar{6}) = \bar{2}$, $\phi(\bar{3}) = \phi(\bar{7}) = \bar{3}$.

Analogt visas att både $\bar{2}$ och $\bar{3}$ i $\mathbb{Z}_4$ är möjliga bilder av $\bar{1} \in \mathbb{Z}_8$.

b) görs analogt med a). Men $\bar{1}$ i $\mathbb{Z}_8$ kan inte avbildas på något element $\neq \bar{0}$ i $\mathbb{Z}_5$. För om $\phi(\bar{1}) = \bar{b} \in \mathbb{Z}_5$, så blir $\phi(8 \cdot \bar{1}) = 8 \cdot \bar{b} \neq \bar{0}$ om $\bar{b} \neq \bar{0}$. Men $\phi(\bar{0}) = \bar{0}$, om ϕ är en homomorfism.

GA 26 f är en homomorfism $\Leftrightarrow (xy)^{-1} = x^{-1}y^{-1}$ för alla $x,y \in G \Rightarrow$ $y^{-1}x^{-1} = x^{-1}y^{-1}$ för alla $x,y \in G \Leftrightarrow xy = yx$ för alla $x,y \in G$.

f är på: för $x \in G$ är $f(x^{-1}) = x$.

f är 1-1: $f(x) = f(y) \Rightarrow x^{-1} = y^{-1} \Rightarrow x = y$.

GA 27 G_1 och G_3 är cykliska, genererade av $\overline{2}$ resp. $\overline{3}$. Avbildningen f från G_1 till G_3 given av att $\overline{1} \to \overline{1}$, $\overline{2} \to \overline{3}$, $\overline{3} \to \overline{7}$, $\overline{4} \to \overline{9}$ är en isomorfism på:

$f(\overline{2} \cdot \overline{2}) = \overline{9}$ och $f(\overline{2}) \cdot f(\overline{2}) = \overline{9}$ $\quad f(\overline{3} \cdot \overline{3}) = \overline{9}$ och $f(\overline{3}) \cdot f(\overline{3}) = \overline{9}$

$f(\overline{2} \cdot \overline{3}) = \overline{1}$ och $f(\overline{2}) \cdot f(\overline{3}) = \overline{1}$ $\quad f(\overline{3} \cdot \overline{4}) = \overline{3}$ och $f(\overline{3}) \cdot f(\overline{4}) = \overline{3}$

$f(\overline{2} \cdot \overline{4}) = \overline{7}$ och $f(\overline{2}) \cdot f(\overline{4}) = \overline{7}$ $\quad f(\overline{4} \cdot \overline{4}) = \overline{1}$ och $f(\overline{4}) \cdot f(\overline{4}) = \overline{1}$.

De produkter där $\overline{1}$ ingår behöver inte kontrolleras, inte heller $f(\overline{ba}) = f(\overline{b})f(\overline{a})$ om $f(\overline{ab}) = f(\overline{a})f(\overline{b})$ kontrollerats.

G_2 och G_4 är också isomorfa: $\overline{1} \to \overline{1}$, $\overline{3} \to \overline{5}$, $\overline{5} \to \overline{7}$, $\overline{7} \to \overline{11}$ t.ex. är en isomorfism (visas på samma sätt som ovan).

Däremot är G_1 och G_2 inte isomorfa: om $\overline{2} \in G_1$ avbildas på $\overline{a} \in G_2$, så skulle $\overline{4} \in G_1$ avbildas på $\overline{a}^2 = \overline{1}$, vilket motsäger en-entydigheten.

GA 31 a) $\mathbb{Z}_5 \ni \overline{a} = \overline{1} + \overline{1} + \ldots + \overline{1}$ (a st) avbildas av en homomorfism $\phi: \mathbb{Z}_5 \to \mathbb{Z}_5$ på $\phi(\overline{1}) + \phi(\overline{1}) + \ldots + \phi(\overline{1}) = a\phi(\overline{1})$.

b) $\overline{1}$ kan inte avbildas på $\overline{0} \in \mathbb{Z}_5$ av en automorfism. $\phi_1: \mathbb{Z}_5 \to \mathbb{Z}_5$ given av att $\phi_1(\overline{1}) = \overline{1}$ är den identiska avbildningen. $\phi_2: \mathbb{Z}_5 \to \mathbb{Z}_5$ given av att $\phi_2(\overline{1}) = \overline{2}$ avbildar $\overline{2}$ på $\overline{4}$, $\overline{3}$ på $\overline{1}$ och $\overline{4}$ på $\overline{3}$; den är 1-1 och på, alltså en automorfism. På samma sätt inses att $\phi_3: \mathbb{Z}_5 \to \mathbb{Z}_5$ given av att $\phi_3(\overline{1}) = \overline{3}$ och $\phi_4: \mathbb{Z}_5 \to \mathbb{Z}_5$ given av att $\phi_4(\overline{1}) = \overline{4}$ är automorfismer.

c) Vi vet att mängden av automorfismer bildar en grupp under sammansättning. Pröva om någon av ϕ_1 - ϕ_4 i b) genererar automorfismgruppen av $\mathbb{Z}_5$. $\phi_2^2(\overline{1}) = \phi_2(\overline{2}) = 2\phi_2(\overline{1}) = \overline{4} \Rightarrow \phi_2^2 = \phi_4$. Analogt visas att $\phi_2^3 = \phi_3$, och klart att $\phi_2^4 = \phi_1 = \text{id}$. ϕ_2 är alltså generator för automorfismgruppen.

d) På samma sätt som i a) inses att varje automorfism av $\mathbb{Z}_6$ är bestämd så snart bilden av $\overline{1}$ är bestämd. Vad kan $\overline{1}$ avbildas på? $\overline{1} \to \overline{1}$ ger förstås den identiska avbildningen. Om $\overline{1} \to \overline{2}$, så $\overline{3} \to 3 \cdot \overline{2} = \overline{0}$, dvs avbildningen blir inte 1-1. Analogt visas att $\overline{1} \to \overline{3}$ resp. $\overline{1} \to \overline{4}$ inte heller ger 1-1 avbildningar. $\overline{1} \to \overline{5} = -\overline{1}$ ger en automorfism (ses direkt eller med GA 26). Det finns alltså två automorfismer av $\mathbb{Z}_6$, den identiska avbildningen och avbildningen som tar varje element till dess invers. Automorfismgruppen för $\mathbb{Z}_6$ är cyklisk av ordning 2.

GA 33 a) Låt G genereras av x, och låt $\phi: G \to G'$ vara en grupphomomorfism på. Vi skall visa att G' genereras av $\phi(x)$. Låt därför g' vara ett godtyckligt element i G'. ϕ på $\Rightarrow g' = \phi(g)$ för något $g \in G$. Men $g = x^k$ för något $k \in \mathbb{Z}$, så $g' = \phi(x^k) = \phi(x)^k$ eftersom ϕ är en homomorfism.

b) $\mathbb{Z}_{17}$ och $\mathbb{Z}_{18}$ är cykliska grupper under addition; homomorfa bilder av dem är alltså cykliska. Vidare är en homomorf bild isomorf med någon faktorgrupp. Z_{17} har bara de triviala delgrupperna $\{0\}$ och $\mathbb{Z}_{17}$, alltså också bara de triviala faktorgrupperna Z_{17} resp. $\{0\}$. $\mathbb{Z}_{18}$:s delgrupper bestämdes i GA 10. De är alla normala. De homomorfa bilderna av $\mathbb{Z}_{18}$ är alltså cykliska grupper av ordning 18, 9, 6, 3, 2, 1 (faktorgrupperna modulo delgrupperna i den ordning de står i svaret till GA 10).

GB 5 a) Det givna villkoret är att $a^{-1} = a$ för alla $a \in G$. Låt nu $a,b \in G$. $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$.

b) Låt $a_1,a_2,..,a_k$ vara en minimal mängd generatorer för G. Varje element g i G kan då skrivas som en produkt av dessa, och de behövs allihop för att varje element i G skall vara en produkt av dem. G abelsk enl. a) $\Rightarrow$ $g = a_1^{i_1}a_2^{i_2}...a_k^{i_k}$, där $i_j = 0,1$ $(j = 1,..,k)$. Eftersom varje exponent kan väljas på två sätt finns högst 2^k sådana produkter. Kan två produkter vara lika för olika exponentmängder? Antag $a_1^{i_1}...a_k^{i_k} = a_1^{j_1}...a_k^{j_k}$ och $i_\nu \neq j_\nu$. Då är $i_\nu = 1$ och $j_\nu = 0$ (eller omvänt). Ur likheten kan vi då lösa ut a_ν: $a_\nu = a_\nu^{i_\nu} = a_1^{i_1}..a_{\nu-1}^{i_{\nu-1}}(a_1^{j_1}..a_{\nu-1}^{j_{\nu-1}}a_{\nu+1}^{j_{\nu+1}}...a_k^{j_k})a_{\nu+1}^{i_{\nu+1}}...a_k^{i_k}$. Men det betyder att varje element i G kan skrivas som en produkt av elementen $a_1,..,a_{\nu-1}$, $a_{\nu+1},..,a_k$, vilket strider mot antagandet. Alltså ger olika exponentmängder olika produkter, varav fås att G har 2^k element.

GB 6 Skriv $m = q\cdot o(a) + r$ med $0 \leq r < o(a)$. $e = a^m = a^{q\cdot o(a) + r} = (a^{o(a)})^q a^r = a^r$. Men $o(a)$ är det minsta positiva heltalet n så att $a^n = e$, så det måste gälla att $r = 0$. Då är $m = q\cdot o(a)$, dvs. $o(a)|m$.

GB 9 Definiera en relation på G: $x \sim y \Leftrightarrow (x = y$ eller $x = y^{-1})$. Klart att den är reflexiv. Den är symmetrisk: $x = y^{-1} \Rightarrow y = x^{-1}$, och transitiv: $(x = y^{-1}$ och $y = z) \Rightarrow x = z^{-1}$ resp. $(x = y^{-1}$ och $y = z^{-1}) \Rightarrow x = z$. Genom denna ekvivalensrelation indelas G i parvis disjunkta ekvivalensklasser, som är av formen $\{x,x^{-1}\}$, om $x \neq x^{-1}$ resp. av formen $\{x\}$, om $x = x^{-1}$. e ligger i en klass för sig. Om inget annat element vore sin egen invers, så skulle $G\setminus\{e\}$ delas upp i parvis disjunkta mängder, som var och en har två element. G skulle då ha $2n + 1$ element för något n. Om G har jämn ordning måste alltså minst ett element $\neq e$ vara sin sin egen invers, så att $G\setminus\{e\}$ innehåller någon klass med ett element.

GB 17 $a \in N \Leftrightarrow Na = N$. Lagranges sats $\Rightarrow o(Na) | o(G/N)$. GB 16 $\Rightarrow$ $o(Na) | o(a)$. Alltså $o(Na) | (o(G/N), o(a)) = 1$, dvs. $o(Na) = 1$. Men då är Na neutralt element i G/N, dvs. $Na = N$.

GB 21 Betrakta avbildningen $f: \mathbb{R} \to \mathbb{R}_+$ given av att $f(x) = 2^x$. Enligt teorin för exponentialfunktioner är den 1-1 och på. Den är också en homomorfism: $f(x+y) = 2^{x+y} = 2^x 2^y = f(x)f(y)$. Alltså är $(\mathbb{R},+)$ och $(\mathbb{R}_+,\cdot)$ isomorfa.

GB 23 $(\mathbb{Z},+)$ har neutralt element = 0 och $(G,*)$ har neutralt element = -10. Pröva avbildningen $f: \mathbb{Z} \to G$ given av att $f(n) = n - 10$. Den avbildar neutralt element på neutralt element. Den är 1-1: $f(n) = f(m) \Rightarrow n = m$ resp. på: för $n \in G$ är $n = f(n + 10)$. Är den en homomorfism?
$f(n + m) = n + m - 10$ och $f(n) * f(m) = (n - 10) * (m - 10) = n - 10 + m - 10 + 10 = n + m - 10$. f är alltså en isomorfism av $(\mathbb{Z},+)$ på $(G,*)$.

GB 24 a) Antag först $o(x) = n < \infty$. $x^n = e \Rightarrow e = f(x^n) = (f(x))^n \Rightarrow$ $o(f(x)) = m < \infty$ och $m | n$ enligt GB 6. Vi har också $e = (f(x))^m = f(x^m)$, vilket medför $x^m = e$ eftersom f är 1-1. Alltså $n | m$, som tillsammans med $m | n$ medför att $m = n$.
Av ovanstående följer också att $o(x) < \infty$ om $o(f(x)) < \infty$.
Om f är en isomorfi, så är alltså $o(x) = o(f(x))$.
b) Om $o(x) < \infty$ så visas på samma sätt som i a) att $o(f(x)) | o(x)$.
I detta fall kan dock gälla att $o(x) = \infty$ och $o(f(x)) < \infty$.
Låt t.ex. G = {inverterbara 2 x 2-matriser} och $\overline{G} = \mathbb{R}_+$ (i båda fallen är operationen multiplikation). $f: G \to \overline{G}$ ges av att $f(A) = \det(A)$. Betrakta $A = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$. $A^k = \begin{pmatrix} 1 & ka \\ 0 & 1 \end{pmatrix}$, så $A^k \neq E$ för alla heltal k, dvs. $o(A) = \infty$. Men $f(A) = 1$, dvs. av ordning 1.

GB 25 Om det finns ett element som är det enda av sin ordning så måste det avbildas på sig själv av varje automorfism enligt GB 24. e är ett sådant. Låt G = (x), o(x) = 58.

Då är

$$o(x^k) = \begin{cases} 58 & \text{om } (58,k) = 1 \\ 29 & \text{om } (58,k) = 2 \\ 2 & \text{om } (58,k) = 29 \end{cases} \qquad 1 \leq k < 58$$

Det finns bara ett k med $(58,k) = 29$, nämligen $k = 29$.

Då är x^{29} det enda elementet av ordning 2 och avbildas alltid på sig självt.

För alla element $\neq e, x^{29}$ finns en automorfism som avbildar elementet på ett annat element. Ta t.ex. $f:G \to G$ given av att $f(x^k) = x^{3k}$.

GB 28 $T = \{z \in \mathbb{C};\ |z| = 1\} = \{e^{ir}; r \in \mathbb{R}\}$. Avbildningen $\mathbb{R} \to T$ given av att $r \to e^{ir}$ är en homomorfism på, men dess kärna är $\{r \in \mathbb{R};\ r = 2\pi n\} \neq \mathbb{Z}$. Vi kan dock modifiera avbildningen. Låt $f:\mathbb{R} \to T$ ges av att $f(r) = e^{2\pi ir}$. f är en homomorfism på, och $\operatorname{Ker} f = \{r \in \mathbb{R};\ e^{2\pi ir} = 1\} = \{r \in \mathbb{R};\ 2\pi r = 2\pi n, n \in \mathbb{Z}\} = \mathbb{Z}$.

GB 30 I S_3 låt $\phi = (1,2)$ och $\psi = (1,2,3)$. ϕ och ψ genererar S_3.

a) Låt T_a vara den inre automorfismen $x \to a^{-1}xa$.

Klart att T_e = identiteten. Vidare är

$$\begin{cases} \phi T_\phi = \phi \\ \psi T_\phi = \psi^2 \end{cases} \quad \begin{cases} \phi T_\psi = \psi\phi \\ \psi T_\psi = \psi \end{cases} \quad \begin{cases} \phi T_{\psi^2} = \phi\psi \\ \psi T_{\psi^2} = \psi \end{cases} \quad \begin{cases} \phi T_{\phi\psi} = \psi\phi \\ \psi T_{\phi\psi} = \psi^2 \end{cases} \quad \begin{cases} \phi T_{\psi\phi} = \phi\psi \\ \psi T_{\psi\phi} = \psi^2 \end{cases}$$

Det finns alltså 6 stycken olika inre automorfismer.

b) S_3 genereras av ϕ och $\psi \Rightarrow$ en automorfism av S_3 är bestämd så snart bilderna av ϕ och ψ är bestämda.

GB 24 $\Rightarrow$ ϕ:s bild är av ordning 2 och ψ:s bild är av ordning 3 $\Rightarrow$ ϕ kan avbildas på $\phi, \phi\psi$ eller $\psi\phi$ och ψ på ψ eller ψ^2. Det finns alltså högst 6 stycken kombinationer av bilder av ϕ och ψ och därmed högst 6 stycken automorfismer av S_3.

c) a) och b) $\Rightarrow$ automorfismgruppen av S_3 = gruppen av inre automorfismer av S_3.

Avbildningen $S_3 \to$ gruppen av inre automorfismer av S_3 given av att $a \to T_a$ är på (klart) och 1-1 (enligt a)).

Den är vidare en homomorfism:

$$xT_{ab} = (ab)^{-1}x(ab) = b^{-1}a^{-1}xab = (a^{-1}xa)T_b = xT_aT_b$$

(här betyder T_aT_b att T_a tas först och sedan T_b. Om man i stället definierar T_aT_b så att T_b tas först och sedan T_a, så får man för att avbildningen $a \to T_a$ skall vara en homomorfism definiera den inre automorfismen T_a så att $x \to axa^{-1}$).

GB 33 a) Låt $\rho = (a_1, a_2, .., a_k)$ vara en k-cykel. Man ser (t.ex. med induktion) att $\rho^s(a_1) = a_{s+1}$ om $1 \leq s < k$, så att $\rho^s \neq e$ om $s < k$. Analogt inses att $\rho^k(a_i) = a_i$ för $1 \leq i \leq k$, varav följer att $o(\rho) = k$.

b) Låt $\rho_1 = (a_1, .., a_{m_1})$, $\rho_2, .., \rho_k$ vara parvis disjunkta cykler av längderna $m_1, m_2, .., m_k$.

Om $m_i | r$ för $i = 1, .., k$, så är $(\rho_1\rho_2..\rho_k)^r = \rho_1^r\rho_2^r..\rho_k^r = e$.

Det betyder att $o(\rho_1\rho_2..\rho_k)$ delar minsta gemensamma multipeln till $m_1, m_2, .., m_k$.

Omvänt: om $s = o(\rho_1\rho_2..\rho_k)$ så är $\rho_1^s\rho_2^s..\rho_k^s = e$. Betrakta talet a_i i cykeln ρ_1. Det avbildas på sig självt av $\rho_1^s\rho_2^s..\rho_k^s$. Det avbildas på sig självt också av cyklerna $\rho_2, .., \rho_k$, liksom av produkter av dessa. Då måste $\rho_1^s(a_i) = a_i$, dvs. $\rho_1^s = e$, varav följer att $m_1 | s$. På samma sätt inses att $m_i | s$ för $i = 2, .., k$, vilket medför att minsta gemensamma multipeln till $m_1, m_2, .., m_k$ delar s. Lösningen är alltså $o(\rho_1\rho_2..\rho_k)$ = minsta gemensamma multipeln till $m_1, m_2, .., m_k$.

OBS! Det är väsentligt att cyklerna är disjunkta. Ty om man betraktar $\phi = (1,2)$ och $\psi = (1,2,3)$ så är $o(\phi\psi) = 2 \neq 6 =$ minsta gemensamma multipeln till 2 och 3.

GB 38 a) se svaret

b) Betrakta a = (1,2), b = (3,4,5), c = (6,7,8,9,10) och d = (3,4). $a = \rho^{15}$, $b = \rho^{10}$, $c = \rho^{6}$, $d = \tau^{5} \Rightarrow a,b,c,d \in H$ $\Rightarrow$ (a,b,c,d) = den delgrupp som genereras av a,b,c,d är innehållen i H.

$\rho = abc$ och $\tau = cd \Rightarrow H \subseteq (a,b,c,d)$. Alltså H = (a,b,c,d).

c) Enligt b) är H mängden av produkter som kan bildas av a,b,c,d. Eftersom a kommuterar med b,c,d och c kommuterar med a,b,d så är varje sådan produkt av formen

$$a^{i}b^{j_1}d^{k_1}\ldots b^{j_n}d^{k_n}c^{l}.$$

Här är $i = 0,1$, $j_t = 0,1,2$, $k_t = 0,1$ och $l = 0,1,2,3,4$.
Hur många element av formen $b^{j_1}d^{k_1}\ldots b^{j_n}d^{k_n}$ finns det?
Antalet = ordningen av den grupp som genereras av b och d. Men den gruppen är isomorf med S_3 (avbilda b på (1,2,3) och d på (1,2)), alltså av ordning 6. I H finns då $2 \cdot 6 \cdot 5 = 60$ element.

GB 39 a) $\tau = \rho^{-1}(a_1,a_2,..,a_k)\rho$ avbildar $\rho(a_1)$ på följande sätt:
$\rho(a_1) \xrightarrow{\rho^{-1}} a_1 \xrightarrow{(a_1,a_2,..,a_k)} a_2 \xrightarrow{\rho} \rho(a_2)$. Analogt visas att τ avbildar $\rho(a_2) \to \rho(a_3),\ldots,\rho(a_k) \to \rho(a_1)$.
Den cykel i τ som innehåller $\rho(a_1)$ är alltså av formen $(\rho(a_1),\rho(a_2),..,\rho(a_k))$.
Om $x \neq \rho(a_i)$ $(i = 1,2,..,k)$ så är $\rho^{-1}(x) \neq a_i$ $(i = 1,2,..,k)$ och x avbildas av τ på följande sätt:

$$x \xrightarrow{\rho^{-1}} \rho^{-1}(x) \xrightarrow{(a_1,a_2,..,a_k)} \rho^{-1}(x) \xrightarrow{\rho} x$$

τ är alltså cykeln $(\rho(a_1),\rho(a_2),..,\rho(a_k))$.

b) Enligt a) kan man ta a så att bilderna av 1,3,4 är resp. 2,3,5 och bilderna av 2,6 resp, 1,4, dvs. a = (1,2)(4,5,6).

c) (1,2)(3,5) jämn $\Rightarrow$ $a^{-1}(1,2)(3,5)a$ jämn för alla a, eftersom a och a^{-1} har samma paritet (dvs. de är båda jämna eller båda udda). (3,5,2,4) däremot är udda och kan inte vara lika med $a^{-1}(1,2)(3,5)$ för något a.

d) Om cykelframställningen av x är $\rho_1\rho_2\ldots\rho_k$ så är $a^{-1}xa = a^{-1}\rho_1 a \cdot a^{-1}\rho_2 a \cdot \ldots \cdot a^{-1}\rho_k a$. Enligt a) är $a^{-1}\rho_i a$ en cykel av samma typ som ρ_i (i = 1,..,k). Av a) följer också att cyklerna $a^{-1}\rho_i a$ (i = 1,..,k) är parvis disjunkta. Om $y = a^{-1}xa$ för något a, så har alltså x och y cykeluppdelningar av samma typ.

Antag omvänt att x och y har cykeluppdelningar av samma typ: $x = \rho_1\rho_2\ldots\rho_k$ och $y = \tau_1\tau_2\ldots\tau_k$ med $o(\rho_i) = o(\tau_i)$ (i = 1,..,k). Låt a vara den permutation som överför elementen i ρ_i i tur och ordning på elementen i τ_i (i = 1,..,k). a är väldefinierad: om $s \neq t$ och s,t finns i några av cyklerna $\rho_1,\rho_2,..,\rho_k$ så är $a(s) \neq a(t)$ eftersom cyklerna $\tau_1,\tau_2,..,\tau_k$ är parvis disjunkta. Olika tal som inte finns med i någon cykel i x avbildas av a på olika tal som inte finns med i någon cykel i y. Detta går bra eftersom x och y lämnar lika många element fixa. Enligt a) är $y = a^{-1}xa$.

GB 40 a) GB 33 $\Rightarrow$ en permutation av ordning 5 har en cykelframställning som bara innehåller 5-cykler. I S_5 kan en permutation innehålla högst en 5-cykel i sin cykelframställning. Alltså är ett element av ordning 5 i S_5 en 5-cykel (a_1,a_2,a_3,a_4,a_5).

b) En delgrupp H av ordning 5 genereras av en 5-cykel (a_1,a_2,a_3,a_4,a_5), dvs. $H = \{(a_1,a_2,a_3,a_4,a_5), (a_1,a_3,a_5,a_2,a_4), (a_1,a_4,a_2,a_5,a_3), (a_1,a_5,a_4,a_3,a_2), e\}$. H är inte normal:

ty ta $x = (a_1,a_2)$. Då är $x^{-1}(a_1,a_2,a_3,a_4,a_5)x = (a_1,a_3,a_4,a_5,a_2) \notin H$.

(Man kan också använda GB 39 d) som ju ger att varje 5-cykel kan skrivas $x^{-1}(a_1,a_2,a_3,a_4,a_5)x$ för något x.)

c) Om S_4 vore homomorf bild av S_5, skulle det enligt homomorfisatsen finnas en normal delgrupp H i S_5 sådan att $S_5/H \simeq S_4$. Lagranges sats $\Rightarrow 120 = o(S_5) = o(H)o(S_4) = o(H)\cdot 24$, vilket ger $o(H) = 5$. Men något sådant H kan inte finnas enligt b).

GC 1 Låt G vara en grupp av ordning 4. Två fall att undersöka:

1) G har element av ordning 4

2) G saknar element av ordning 4.

I 1) är gruppen cyklisk: $G = \{e,a,a^2,a^3;a^4 = e\}$ och kompositionen är bestämd av att $a^i a^j = a^{i+j}$. En sådan grupp existerar också; ta t.ex. $(\mathbf{Z}_4,+)$.

I fall 2) är alla element $\neq e$ av ordning 2, så gruppen abelsk enligt GB 5. Vi får $G = \{e,a,b,ab;\ a^2 = b^2 = e,\ ba = ab\}$ och kompositionstabellen är entydigt given av villkoren på a och b. Det existerar grupper av denna typ, t.ex. $(\mathbf{Z}_8,\cdot)$.

GC 2 Låt G vara en grupp av ordning 6. Två fall att undersöka:

1) G har element av ordning 6

2) G saknar element av ordning 6.

I fall 1) är gruppen cyklisk med entydigt definierad komposition. Fall 2)? GB 9 $\Rightarrow$ det finns element a av ordning 2 i G. GB 5b) $\Rightarrow$ inte alla element är av ordning 2 $\Rightarrow$ det finns ett element b av ordning 3 i G. Då är $G = \{e,a,b,b^2,ab,ab^2\}$. Vilket av dessa element är ba? Klart att $ba \neq e,a,b,b^2$. $ba = ab \Rightarrow o(ab) = 6$, vilket strider mot antagandet i 2). Återstår $ba = ab^2$. Med detta villkor kan en kompositionstabell för $\{e,a,b,b^2,ab,ab^2\}$ bara konstrueras på ett enda sätt. S_3 är ett exempel på en grupp av denna typ.

GC 5 a) Elementen i G är av formen $x^{i_1}y^{j_1}x^{i_2}y^{j_2}\ldots x^{i_n}y^{j_n}$, där $i_k \in \{0,1,\ldots,5\}$ och $j_k \in \{0,1\}$. Med hjälp av villkoret $yx = x^5y$ kan de potenser av x som står till höger om ett y flyttas så att slutligen alla x samlats till vänster, alla y till höger; t.ex. $yx^2 = x^5yx = x^{10}y = x^4y$. Alltså är alla element i G av formen x^iy^j där $i \in \{0,1,\ldots,5\}$ och $j \in \{0,1\}$.

b) Man kan pröva sig fram på olika sätt. Ett sätt är att observera att symmetrigrupperna av en liksidig triangel resp. en kvadrat är uppbyggda analogt: $\{x^i y^j;\ i = 0,1,2 \text{ och } j = 0,1,\ x^3 = y^2 = e,\ yx = x^2y\}$ resp. $\{R_1^i V^j;\ i = 0,1,2,3 \text{ och } j = 0,1,\ R_1^4 = V^2 = I,\ VR_1 = R_1^3 V\}$. I vårt fall, pröva med symmetrier av en regelbunden sexhörning. Numrera hörnen från 1 till 6. Ta x = rotation 1/6 varv = (1,2,3,4,5,6) och y = spegling i diagonalen genom 1 och 4 = (2,6)(3,5). En mera osystematisk prövning ger att man kan ta t.ex. x = (1,2,3)(4,5) och y = (1,2).

GC 6 Den avbildning som tar Ha till aH är inte väldefinierad: betrakta i S_3 $H = \{(1),(1,2)\}$. Då är $H(1,3) = H(1,2,3)$ men $(1,3)H \neq (1,2,3)H$. Pröva i stället den avbildning som tar Ha till $a^{-1}H$. Vi får: $Ha = Hb \Leftrightarrow ab^{-1} \in H \Leftrightarrow (b^{-1})^{-1}a^{-1} = (ab^{-1})^{-1} \in H \Leftrightarrow b^{-1}H = a^{-1}H$. Klart att avbildningen är på. Att den är 1-1 följer om man går från höger till vänster i ekvivalenskedjan ovan.

GC 7 a) (i) c = e ger reflexivitet; (ii) symmetrin följer av att $b = c^{-1}ac \Rightarrow a = cbc^{-1} = (c^{-1})^{-1}bc^{-1}$ och (iii) transitiviteten av att $b = x^{-1}ax$ och $c = y^{-1}by \Rightarrow c = y^{-1}x^{-1}axy = (xy)^{-1}a(xy)$.

b) Ekvivalensklassen till a har ett enda element om och endast om $c^{-1}ac = a$ för alla $c \in G$, dvs om och endast om $ac = ca$ för alla $c \in G$.

c) $\{c^{-1}ac;\ c \in G\} \to \{\text{högersidoklasser till } N_a\}$ given av att $c^{-1}ac \to N_a c$ är väldefinierad: $c^{-1}ac = d^{-1}ad \Rightarrow cd^{-1}a = acd^{-1} \Rightarrow cd^{-1} \in N_a \Rightarrow N_a c = N_a d$. Avbildningen är också 1-1 och på. Vi får alltså antalet element i a:s konjugatklass = index för N_a, som delar o(G) enligt Lagranges sats.

d) Vi får $a_o = p^n - a_1 p - \ldots - a_{n-1}p^{n-1}$, så att $p \mid a_o$, varför $a_o > 1$.

GC 9 $mn = nm \Leftrightarrow mnm^{-1}n^{-1} = e$. N normal delgrupp $\Rightarrow mnm^{-1} \in N$, varav följer $mnm^{-1}n^{-1} \in N$. På samma sätt fås $mnm^{-1}n^{-1} \in M$. $M \cap N = \{e\} \Rightarrow mnm^{-1}n^{-1} = e$.

GC 10 $H = \{g_1^2 g_2^2 \ldots g_k^2;\ g_i \in G\}$. Om $x \in G$, så är $x(g_1^2 g_2^2 \ldots g_k^2)x^{-1} =$
$= (xg_1x^{-1})^2(xg_2x^{-1})^2 \ldots (xg_kx^{-1})^2$, dvs ett element i H. Alltså är H normal. I G/H gäller att $(Ha)^2 = Ha^2 = H$ för varje $a \in G$ eftersom $a^2 \in H$. G/H är då abelsk enligt GB 5.

GC 11 Låt K vara kommutatordelgruppen.

a) se ledningen till GC 11 och lösningen till GC 10.

b) I G/K är $KxKyKx^{-1}Ky^{-1} = Kxyx^{-1}y^{-1} = K$, så att $KxKy = KyKx$.

c) G/H abelsk $\Rightarrow HxHy = HyHx$ för alla $x,y \in G \Rightarrow HxHyHx^{-1}Hy^{-1} = H$ för alla $x,y \in G \Rightarrow xyx^{-1}y^{-1} \in H$ för alla $x,y \in G \Rightarrow K \in H$.

GC 12 Ett godtyckligt element i G är av formen $x = a^{i_1}b^{j_1}a^{i_2}b^{j_2}\ldots a^{i_r}b^{j_r}$.
Ett element i G/N är då av formen $Nx = (Na)^{i_1}(Nb)^{j_1}\ldots(Na)^{i_r}(Nb)^{j_r}$.
a) $ab \in N \Rightarrow Na = (Nb)^{-1} \Rightarrow Nx = (Nb)^{j_1+\ldots+j_r-i_1-\ldots-i_r}$, så att varje element i G/N är en potens av Nb.
I b) är $Nb = (Na)^{-2}$, vilket ger att varje element i G/N är en potens av Na. I c) är varje element i G/N en potens av Nb eftersom $Na = (Nb)^{-2}$.

GC 14 G har ett element a av ordning 2 enligt GB 9. Sätt $H_2 = \{e,a\}$.
$\overline{G} = G/H_2$ är abelsk av ordning 6. Den har då också en delgrupp $\overline{H}$ av ordning 2. $\overline{H} = H_1/H_2$ för någon delgrupp H_1 av G. $H_1 \supseteq H_2$, $\overline{H} \neq \overline{e}$
$\Rightarrow H_1 \neq H_2$ och $\overline{H} \neq \overline{G} \Rightarrow H_1 \neq G$.

GC 15 a) Ta m_1n_1 och m_2n_2 i MN. $Nm_2 = m_2N \Rightarrow$ det finns $n_3 \in N$ så att $n_1m_2 = m_2n_3$ varav följer att $m_1n_1m_2n_2 = (m_1m_2)(n_3n_2) \in MN$.
Analogt visas att $(mn)^{-1} = n^{-1}m^{-1} \in MN$.
$n = e$ ger $M \subseteq MN$.

b) $N \to MN/M$ given av att $n \to M(en) = Mn$ är en grupphomomorfism.
Den är på, ty $M(mn) = Mn$. Kärnan $= \{n \in N;\ Mn = M\} = \{n \in N;\ n \in M\} = M \cap N$.

GC 17 Låt G vara en icke-cyklisk abelsk grupp av ordning p^2.

Lagranges sats $\Rightarrow$ varje element $\neq e$ är av ordning p. Låt x vara ett element av ordning p. Ta $y \in G \setminus (x)$. y är av ordning p och $(y) \cap (x) = (e)$. Ty antag $y^r = x^s$ för r,s båda $\neq p$. Då är $o(y^r) = p$, så $(y^r)^t = y$ för något t, varav fås $y = x^{st}$, en motsägelse mot $y \notin (x)$. Alltså är $G = \{x^i y^j;\ i,j = 0,1,\ldots,p-1\}$.

Om G' är en annan icke-cyklisk abelsk grupp av ordning p^2, genererad av z och w av ordning p, så får en isomorfism av G på G' av att $x \to z, y \to w$.

GC 18 Sätt $o(G) = 2n + 1$. Då är $g^{2n+1} = e$ för alla $g \in G$. Den givna avbildningen är 1-1: $g^2 = h^2 \Rightarrow g^{2n+1} = h^{2n+1} = g^{2n}h \Rightarrow g = h$. Enligt I 4 är den då också på. Den är en homomorfism om och endast om G är abelsk enligt GA 8.

Uppgifter

RA 1 Vilka av följande mängder är ringar med sina naturliga additioner och multiplikationer?

a) Mängden av jämna hela tal.

b) Mängden av udda hela tal.

c) Mängden av positiva hela tal.

d) Mängden av 2X2-matriser med reella tal som koefficienter.

e) Mängden av 2X2-matriser med hela tal som koefficienter.

f) Mängden av 2X2-matriser med determinant skild från noll med reella tal som koefficienter.

RA 2 Vilka av ringarna i ovanstående exempel har en etta? Vilka är kommutativa? Vad heter nollelementet?

RA 3 Visa att $\{x+y\sqrt[3]{3}+z\sqrt[3]{9}: x,y,z \in Q\}$ med vanlig addition och multiplikation är en ring.

RA 4 Visa att mängden av reellvärda funktioner på reella axeln med vanlig addition och multiplikation blir en ring. Har ringen etta? Bestäm nollelementet. Finns något element $f(x) \neq$ nollelementet så att $f(x)\cdot x =$ nollelementet i ringen? Vilka element är nolldelare i ringen?

RA 5 Mängden M = {a,b,c,d} med nedanstående addition och multiplikation är en ring.

+	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

·	a	b	c	d
a	a	a	a	a
b	a	b	a	b
c	a	c	a	c
d	a	d	a	d

a) Vilket är nollelementet?

b) Vilka är elementens additiva inverser?

c) Har ringen etta?

d) Är ringen kommutativ?

e) Har ringen nolldelare?

f) Är {a,b} delring till M?

g) Är {a,b,c} delring till M?

RA 6 Ett element i en ring med etta kallas invertibelt om det har en tvåsidig multiplikativ invers.

a) Visa att ett invertibelt element inte kan vara nolldelare.

b) Om a och b är invertibla så är ab invertibel. Visa detta och bestäm inversen till ab.

c) Visa att mängden av invertibla element bildar en multiplikativ grupp.

RA 7 Visa att om a är ett invertibelt element i en ring, så är -a också invertibelt. Vilken är inversen till -a?

RA 8 För ett element x i ett integritetsområde gäller $x^n = 0$. Visa att $x = 0$.

RA 9 Låt A och B vara ringar. Definiera den direkta summan $A \oplus B$ som mängden av alla par (a,b), där $a \in A$, $b \in B$. Sätt $(a_1,b_1) + (a_2,b_2) = (a_1 + a_2, b_1 + b_2)$ och $(a_1,b_1)\cdot(a_2,b_2) = (a_1a_2,b_1b_2)$.

a) Visa att $A \oplus B$ är en ring.

b) Kan $A \oplus B$ vara ett integritetsområde?

RA 10 Utveckla $(a + b)^3$ i en godtycklig ring.

RA 11 R är en ring, $x,y \in R$. Sätt $[x,y] = xy - yx$. Visa att $[x,[y,z]] + [y,[z,x]] + [z,[x,y]] = 0$.

RA 12 Låt G vara en additiv abelsk grupp. Definiera $a\cdot b = 0$ för varje $a,b \in G$. Visa att G blir en ring.

RA 13 Om för två element a,b i en ring gäller ab = ba så gäller också a(-b) = (-b)a. Visa detta.

RA 14 Visa att $\{\begin{pmatrix} a & 2b \\ 0 & a \end{pmatrix}: a,b \in Z\}$ är en delring till ringen av 2X2-matriser med koefficienter i Z.

RA 15 Visa att $\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix}: a,b \in \mathbb{R}\}$ är en delring till ringen av 2X2-matriser

med reella koefficienter.

RA 16 Låt R vara mängden av alla delmängder till en given mängd S. Definiera addition i R genom $A + B = (A \cup B) \setminus (A \cap B)$ och multiplikation genom $A \cdot B = A \cap B$

a) Visa att R blir en ring.

b) Är R kommutativ?

c) Har R etta?

RA 17 a) Visa att $N = \{(a,b,c,d): a,b,c,d \in C\}$ med additionen $(a,b,c,d) + (e,f,g,h) = (a + e, b + f, c + g, d + h)$ och multiplikationen $(a,b,c,d)\cdot(e,f,g,h) = (ae + bg, af + bh, ce + dg, cf + dh)$ är en ring.

b) Vilket är nollelementet?

c) Vilken är den additiva inversen till elementet (a,b,c,d)?

d) Visa att ringen har etta. Vilken?

e) Vilka element har multiplikativ invers?

f) Är ringen kommutativ?

g) Visa att delmängden $P = \{(a,b,-b,a): a,b \in Z\}$ är en delring.

h) Är P kommutativ?

i) Visa att delmängden $R = \{(z_1,z_2,-\bar{z}_2,\bar{z}_1)\}$ är en delring.

j) Är R kommutativ?

k) Visa att alla element i R utom nollelementet har en multiplikativ invers. Vilken är inversen till $(z_1,z_2,-\bar{z}_2,\bar{z}_1)$?

RA 18 Låt R vara en ring. På $RXZ = \{(r,z): r \in R, z \in Z\}$ definieras en addition genom $(r,m) + (s,n) = (r + s, m + n)$ och en multiplikation genom $(r,m)\cdot(s,n) = (rs + nr + ms, mn)$.

a) Visa att RXZ blir en ring.

b) Vilket är nollelementet?

c) Har ringen etta?

RA 19 Låt f vara en homomorfi av en ring R på en ring S.

a) Visa att om R är kommutativ så är S kommutativ.

b) Visa att om R har en etta så har S en etta och ettan i S är bild av ettan i R.

c) Om R är ett integritetsområde, måste då S vara ett integritetsområde?

RA 20 Låt $Q(\sqrt{2}) = \{a + b\sqrt{2}: a,b \in Q\}$ och $Q(\sqrt{3}) = \{a + b\sqrt{3}: a,b \in Q\}$. Dessa är ringar under vanlig addition och multiplikation av reella tal.

a) Är $Q(\sqrt{2})$ och $Q(\sqrt{3})$ isomorfa som additiva grupper?

b) Är $Q(\sqrt{2})$ och $Q(\sqrt{3})$ isomorfa som ringar?

RA 21 Låt $A \oplus B$ vara en ring som i uppgift RA 9. Definiera en avbildning f från $A \oplus B$ till B genom $f((a,b)) = b$.

a) Visa att f är en homomorfism.

b) Vad är kärnan till denna homomorfism?

RA 22 Visa att $f(a + ib) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ är en isomorfism av de komplexa talen på $\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix}: a,b \in R\}$.

RA 23 Visa att $f(z) = \bar{z}$ är en automorfism av C.

RA 24 a) Visa att $f(\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}) = a$ är en homomorfism av diagonalmatriserna av typ 2X2 med reella koefficienter till R.

b) Är det en isomorfism?

RA 25 Låt f vara en automorfism av en ring. Visa att de element a, för vilka gäller $f(a) = a$ bildar en delring.

RA 26 Låt P vara ringen i uppgift RA 17 g. En avbildning f från P till Z definieras genom $f((a,b,-b,a)) = a$.

a) Är f en homomorfism av de additiva grupperna?

forts.

RA 26 b) Är f en isomorfism av de additiva grupperna?

c) Är f en ringhomomorfism?

RA 27 a) Visa att $N_1 = \{(a,0,c,d): a,c,d \in C\}$ och $N_2 = \{(a,0,0,d): a,d \in C\}$ är delringar av ringen N i uppgift RA 17 a.

b) Visa att f((a,0,c,d)) = (a,0,0,d) är en homomorfism.

c) Bestäm ker f.

d) Är f en isomorfism?

RA 28 Låt RXZ vara en ring som i uppgift RA 18.

a) Visa att RX{0} är ett ideal.

b) Visa att f(x) = (x,0) är en homomorfism av R på RX{0}.

c) Är det en isomorfism?

d) Bestäm RXZ/RX{0}.

RA 29 a) Bestäm största gemensamma delare till 156 och 91 med Euklides algoritm.

b) Skriv den största gemensamma delaren som en linjärkombination av 156 och 91 med hela tal som koefficienter.

RA 30 a) Visa att om två heltal a och b är relativt prima (har största gemensamma delare = 1) så finns $m,n \in Z$ så att 1 = ma + nb.

b) Visa att om 1 = ma + nb, där $m.n.a.b \in Z$ så är a och b relativt prima.

RA 31 Finns det heltal m och n så att

a) 18m + 12n = 6?

b) 18m + 12n = 24?

c) 18m + 12n = 25?

RA 32 Finns det $m,n \in Z$ så att

a) 5m + 16n = 1?

b) 14m + 21n = 1?

RA 33 A är ett ideal i Z sådant att $24 \in A$ och $52 \in A$. Visa att $4 \in A$.

RA 34 Låt $A = \{4m + 6n: m,n \in Z\}$. Visa att A är idealet 2Z.

RA 35 Vilket ideal i Z är $\{6m + 9n: m,n \in Z\}$?

RA 36 Vilket ideal i Z är $\{6a + 12b + 15c: a,b,c \in Z\}$?

RA 37 Vilket ideal i Z är $\{6a + 4b + 14c: a,b,c \in Z\}$?

RA 38 För två ideal i Z gäller $aZ \subseteq bZ$. Vad kan man säga om a och b?

RA 39 A och B är två ideal i Z.

a) När är $A \cup B$ ett ideal?

b) När är $A \cap B$ ett ideal?

RA 40 Låt G vara en ring som i uppgift RA 12. Vilka är idealen?

RA 41 R är en ring med etta, A är ett ideal i R.

a) Visa att $A = R$ om och endast om $1 \in A$.

b) Visa att $A = R$ om och endast om A innehåller ett invertibelt element (definierat i uppgift RA 6).

RA 42 R är en ring, n ett heltal.

Visa att $R_n = \{r \in R: nr = 0\}$ är ett ideal i R.

RA 43 A är ett ideal i en ring R. Visa att $\{x \in R: xa = 0$ för varje $a \in A\}$ är ett ideal.

RA 44 A och B är ideal i en ring R. Definiera $A + B = \{a + b: a \in A, b \in B\}$.

a) Visa att A + B är ett ideal.

b) Visa att $A \subseteq A + B$ och att $B \subseteq A + B$.

c) Låt $A = 4Z$, $B = 6Z$, $R = Z$. Bestäm $d \in Z$ så att $A + B = dZ$.

d) Låt $A = mZ$, $B = nZ$, $R = Z$. Bestäm $d \in Z$ så att $A + B = dZ$.

RA 45 A och B är ideal i en ring R.

a) Visa att $A \cap B$ är ett ideal.

Definiera AB som mängden av ändliga summor av element ab där $a \in A$ och $b \in B$.

b) Visa att AB är ett ideal.

c) Visa att $AB \subseteq A \cap B$.

d) Låt A = 4Z, B = 6Z, R = Z. Bestäm $d \in Z$ så att AB = dZ.

e) Låt A = 4Z, B = 6Z, R = Z. Bestäm $d \in Z$ så att $A \cap B$ = dZ.

f) Låt A = mZ, B = nZ, R = Z. Bestäm $d \in Z$ så att AB = dZ.

g) Låt A = mZ, B = nZ, R = Z. Bestäm $d \in Z$ så att $A \cap B$ = dZ.

RA 46 A, B och C är ideal i en ring R. Definiera $A:B = \{x \in R: xb \in A$ för varje $b \in B\}$.

a) Visa att A:B är ett ideal.

b) Visa att $A \subseteq A:B$.

c) Visa att $(A \cap B):C = (A:C) \cap (B:C)$.

d) Låt A = 4Z, B = 2Z, R = Z. Bestäm $d \in Z$ så att A:B = dZ.

e) Låt A = 4Z, B = 3Z, R = Z. Bestäm $d \in Z$ så att A:B = dZ.

f) Låt A = mZ, B = nZ, R = Z. Bestäm $d \in Z$ så att A:B = dZ.

RA 47 A är ett ideal i en kommutativ ring R. Definiera $N(A) = \{x \in R: x^n \in A$ för något $n\}$.

a) Visa att N(A) är ett ideal (radikalen till A).

b) Visa att $A \subseteq N(A)$.

c) Visa att N(N(A)) = N(A).

d) Låt A = 4Z, R = Z. Bestäm $d \in Z$ så att N(A) = dZ.

e) Låt A = 12Z, R = Z. Bestäm $d \in Z$ så att N(A) = dZ.

f) Låt A = mZ, R = Z. Bestäm $d \in Z$ så att N(A) = dZ.

RA 48 a) Är delringen $\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}: a,b \in Z\}$ ett ideal i ringen av 2X2-matriser med koefficienter i Z?

b) Är $\{\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}: a,b \in Z\}$? tt ideal i samma ring?

RA 49 R är en ring, $a \in R$.

a) Visa att $aR = \{ar: r \in R\}$ är ett ideal om R är kommutativ.

b) Visa att detta inte behöver vara sant om R inte är kommutativ.

c) Visa att aR är det minsta ideal i R som innehåller a om R är kommutativ och har etta.

d) Visa att detta inte är sant om R saknar etta.

e) Vilka element ingår i det minsta ideal som innehåller a om R är kommutativ? Om R är ickekommutativ?

RA 50 Om R är en ring och L en delmängd till R kallas L vänsterideal om L är en additiv delgrupp till R och om $\{rl: r \in R, l \in L\} \subset L$. (Analogt definieras högerideal.)

a) Visa att aR i uppgift RA 49a alltid är ett högerideal.

b) Visa att delringen i uppgift RA 48a är ett högerideal.

c) Visa att delringen i uppgift RA 48b är ett vänsterideal.

d) Är delringen {a,b} i uppgift RA 5 ett ideal i M? Ett högerideal? Ett vänsterideal?

RA 51 Är $\{\begin{pmatrix} m-2n & n \\ 2m-4n & 2n \end{pmatrix}: m,n \in Z\}$ ett ideal i ringen av 2X2-matriser med koefficienter i Z? Ett högerideal? Ett vänsterideal?

RA 52 Ett ideal P i en kommutativ ring R kallas primideal om $ab \in P$ medför $a \in P$ eller $b \in P$.

a) Visa att P är ett primideal om och endast om R/P saknar nolldelare.

b) Bestäm primidealen i Z.

c) Visa att om R har en etta så är maximalidealen i R primideal.

d) Ge exempel på att detta inte behöver vara sant om R saknar etta.

forts.

RA 52 e) Låt f vara en homomorfism av R på en ring S. Visa att maximalidealen (resp. primidealen) i R som omfattar kärnan till f svarar mot maximalidealen (resp. primidealen) i S.

f) Visa att om P är ett primideal så är N(P) = P. (N(P) är definierat i uppgift RA 47.)

RA 53 R är ett integritetsområde, a och b är element i R skilda från noll. Visa att aR = bR om och endast om a och b är associerade.

RA 54 Visa att $Z[X]/(3,2X^2 + 1)$ är isomorf med $Z_3[X]/(\bar{2}X^2 + \bar{1})$.

RA 55 Bestäm summa och produkt av

a) $\bar{4} + X + \bar{2}X^2$ och $\bar{1} + \bar{2}X + \bar{3}X^2$ i $Z_5[X]$.

b) $\bar{2} + \bar{2}X + X^3$ och $\bar{1} + X + X^2 + X^4$ i $Z_3[X]$.

RA 56 Gör additions- och multiplikationstabell för $Z_2[X]/(X^2 + X + 1)$.

RA 57 a) Bestäm största gemensamma delare till $X^3 + 2X^2 + X + 2$ och $X^3 + 3X^2 + 3X + 2$ i $Q[X]$. Skriv sedan denna som $f(X)(X^3 + 2X^2 + X + 2) + g(X)(X^3 + 3X^2 + 3X + 2)$, $f(X)$, $g(X) \in Q[X]$.

b) Samma uppgift för $X^3 + X$ och $X^3 + X^2 + X + \bar{1}$ i $Z_2[X]$.

RA 58 Bestäm alla primpolynom av grad ≤ 3 i $Z_2[X]$.

RA 59 Bestäm antalet primpolynom av grad 2 i $Z_p[X]$, p primtal.

RA 60 Visa att $\bar{3}X^3 + \bar{4}X^2 + \bar{3} = (X + \bar{2})^2(\bar{3}X + \bar{2}) = (X + \bar{2})(X + \bar{4})(\bar{3}X + \bar{1})$ i $Z_5[X]$. Varför strider inte detta mot den entydiga faktoriseringen?

RA 61 Uppdela primfaktorer

a) $X^4 + X^3 + X^2 + \bar{1}$ i $Z_2[X]$.

b) $X^4 + X^2 + \bar{1}$ i $Z_2[X]$.

c) $X^4 + \bar{2}X + \bar{2}$ i $Z_5[X]$.

d) $\bar{4}X^4 + \bar{3}X^3 + \bar{4}X^2 + \bar{4}X + \bar{6}$ i $Z_7[X]$.

RA 62 Visa att polynomen X och X^5 antar samma värden för varje $a \in Z_5$.

RA 63 a) Visa att $Q[X]/(X^2 - 3)$ är isomorf med $Q(\sqrt{3}) = \{a + b\sqrt{3}: a,b \in Q\}$.

b) Visa att $\mathbb{R}[X]/(X^2 + 1)$ är isomorf med C.

RA 64 Faktorisera i $Q[X]$, $\mathbb{R}[X]$ och $C[X]$

a) $X^4 - 1$

b) $4X^5 + 4X^4 - 13X^3 - 11X^2 + 10X + 6$.

RA 65 R är ett integritetsområde

a) Visa att $R[X]$ är ett integritetsområde.

b) Visa att $R[X]$ inte är en kropp, om inte R är nollring.

RA 66 a) Visa att $X^3 - X$ har 6 nollställen i Z_6.

b) Visa att $X^2 + e$ har oändligt många nollställen i de reella quaternionerna. (Se RB 12.)

Uppgifter

RB 1 a) Visa att mängden av endomorfismer (homomorfismer av en grupp in i sig själv) av en abelsk grupp bildar en ring under följande operationer:

$\phi + \psi$ är den endomorfism, som definieras av $(\phi + \psi)(x) = \phi(x) + \psi(x)$.

$\phi \cdot \psi$ definieras av $(\phi \cdot \psi)(x) = \phi(\psi(x))$.

b) Bestäm endomorfismringen till en oändlig cyklisk grupp.

c) Bestäm endomorfismringen till en ändlig cyklisk grupp.

d) Bestäm endomorfismringen till additiva rationella talgruppen.

RB 2 Ett ringelement x kallas idempotent om det uppfyller $x^2 = x$. Avgör om en kommutativ ring med enhetselement kan innehålla

a) andra inverterbara idempotenter än 1

b) andra idempotenter överhuvud taget än 1 och 0.

RB 3 a) Fullständiga multiplikationstabellen för följande ring

+	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

·	a	b	c	d
a	a	a	a	a
b	a	b		
c	a			a
d	a	b	c	

b) Är ringen kommutativ?

c) Har ringen etta?

RB 4 a) Fullständiga multiplikationstabellen för följande ring

+	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

·	a	b	c	d
a				
b		b		
c				c
d		b	c	

b) Är ringen kommutativ?

c) Har ringen etta?

RB 5 R är en ändlig ring med etta, G är delmängden av element i R som inte är nolldelare. Visa att G är en multiplikativ grupp.

RB 6 Bestäm gruppen G i ovanstående uppgift, om $R = Z_n$.

RB 7 Ett element a i en ring kallas nilpotent om det finns ett n så att $a^n = 0$.

a) Visa att om a är nilpotent i en ring med etta, så har 1 - a invers.

b) Visa att i en kommutativ ring R bildar mängden av nilpotenta element ett ideal.

c) Beteckna ovanstående ideal med N. Visa att 0 är det enda nilpotenta elementet i R/N.

RB 8 Visa att i en ring A är det ideal som genereras av alla element av typen $xy - yx$, där $x,y \in A$, det minsta ideal B sådant att A/B är kommutativ.

RB 9 Låt p och q vara olika primtal. Bestäm så när som på isomorfism de ringar som kan vara homomorfa bilder av Z_{pq}.

RB 10 a) Vilka delringar av Z kan vara homomorfa bilder av Z?

b) Samma fråga för Q.

RB 11 p är ett primtal. Låt R vara den delmängd av de rationella talen, som består av de tal som kan skrivas a/b där (b,p) = 1.

a) Visa att R är en delring av Q.

b) Visa att för varje $x \in Q$ gäller $x \in R$ eller $x^{-1} \in R$.

c) Visa att för varje $x \in Q$, $x \neq 0$ finns ett entydigt $n \in Z$ så att $x = p^n u$, där u är ett invertibelt element i R.

d) Visa att de enda delringar av Q som omfattar R, är R och Q.

e) Vilka är de invertibla elementen i R?

f) Vilka ideal finns i R?

RB 12 Låt K vara kroppen av rationella eller reella tal. Bilda ett fyrdimensionellt vektorrum över K med baselementen e, j, k och l.

Definiera en produkt genom:

$ee = e$, $jj = kk = ll = -e$

$ej = je = j$, $ek = ke = k$, $el = le = l$

$jk = l$, $kj = -l$

$kl = j$, $lk = -j$

$lj = k$, $jl = -k$

och fortsätt denna multiplikation linjärt.

a) Visa att man får en ickekommutativ ring med etta, där varje element $\neq 0$ har en invers (quaternionerna).

b) Visa att mängden av komplexa matriser $\begin{pmatrix} a+ib & c+id \\ -c+id & a-ib \end{pmatrix}$ med de vanliga räknereglerna bildar en ring, isomorf med den tidigare.

RB 13 Bestäm alla heltal $a > 0$ sådana att $Z/(a)$ har exakt ett ideal utom nollidealet och ringen själv.

RB 14 a) Visa att följande mängder av restklasser är kroppar:

1) $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4},$ modulo 5$\}$

2) $\{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8},$ modulo 10$\}$

b) Undersök om kropparna är isomorfa.

RB 15 a) Visa att $\{\begin{pmatrix} \bar{0} & \bar{0} \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} \bar{1} & \bar{0} \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} \bar{0} & \bar{0} \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} \bar{1} & \bar{0} \\ 1 & 0 \end{pmatrix}: \bar{0}, \bar{1} \in Z_2\}$ är en delring av ringen av 2X2-matriser med koefficienter i Z_2.

b) Visa att mängden i RA 5 är en ring genom att visa att den är isomorf med ovanstående ring.

RB 16 Låt A vara en ring med etta, här betecknad med e. Låt h vara en homomorfism av gruppen Z på gruppen A (i båda fallen med addition som gruppoperation) sådan att dessutom $h(1) = e$.

a) Visa att h också är en homomorfism av ringen Z på ringen A.

b) Visa att ringen A är isomorf med ringen Z eller med ringen $Z/(n)$ för något n.

RB 17 a) På Z definieras kompositionsreglerna $*$ och $\circ$ genom $n * m = n + m + 1$ och $n \circ m = n \cdot m + n + m$. Visa att $(Z, *, \circ)$ är en ring isomorf med den vanliga $(Z, +, \cdot)$.

b) Kan Z ersättas av en godtycklig ring med etta?

RB 18 Låt R vara en ring med etta sådan att den additiva gruppen av R är en ändlig cyklisk grupp. Visa att R är ringisomorf med $Z/(n)$ för något $n \in Z$.

RB 19 $R = \{\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}: a,b \in Q\}$ är en delring av ringen av 2X2-matriser med koefficienter i Q. Visa att $M = \{\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}: b \in Q\}$ är ett maximalideal i R.

RB 20 Bestäm maximalidealen i ringen i RB 11.

RB 21 a) Visa att ringen i RB 11 är euklidisk.

b) Bestäm primelementen i denna ring.

RB 22 Låt R vara ringen av jämna heltal.

a) Vilka primelement finns i R?

b) Är R en euklidisk ring?

c) Visa att varje ideal i R är principalt.

RB 23 Primfaktoruppdela i $Z[i]$

a) $7i - 4$

b) $9 + 4i$

c) $27 + 34i$

d) 31

e) 53

RB 24 Bestäm största gemensamma delare till a och b och skriv den på formen $sa + tb$, med $s,t \in Z[i]$, om

a) $a = 6 + 2i$, $b = 9 - 2i$

b) $a = 2 + i$, $b = 2 - i$

c) $a = 5$, $b = 7 + i$

RB 25 Bestäm det ideal som genereras av a och b i resp. uppgifter ovan.

RB 26 Bestäm idealen $(a) \cap (b)$ i uppgift RB 24.

RB 27 a) Visa att $Z[i]/(2 + i)$ är en kropp.

b) Vilken är karaktäristiken i denna kropp?

c) Hur många element har kroppen?

d) Bestäm inversen till den restklass som representeras av $2 - i$.

RB 28 a) Visa att $Z[i]/3$ är en kropp.

b) Vilken är karaktäristiken?

c) Hur många element har kroppen?

d) Bestäm inversen till den restklass som representeras av $3 + i$.

RB 29 a) Visa att $Z[i]/(5 + 12i)$ inte är någon kropp.

b) Visa att den restklass som representeras av $3 + i$ är invertibel i denna ring och bestäm inversen.

RB 30 Bestäm ett maximalideal i $Z[i]$ som omfattar

a) (2)

b) (5)

RB 31 Låt $Z[\sqrt{-2}] = \{a + b\sqrt{-2}: a,b \in Z\}$. Definiera normen av ett element i $Z[\sqrt{-2}]$ genom $N(a + ib\sqrt{2}) = a^2 + 2b^2$.

a) Visa att $N(xy) = N(x)N(y)$ då $x,y \in Z[\sqrt{-2}]$.

b) Bestäm de invertibla elementen i $Z[\sqrt{-2}]$.

c) Ge exempel på ett primelement i $Z[\sqrt{-2}]$.

d) Visa att $Z[\sqrt{-2}]$ är en Euklidisk ring.

RB 32 Låt $Z[\sqrt{-3}] = \{a + b\sqrt{-3}: a,b \in Z\}$. Definiera normen av ett element i $Z[\sqrt{-3}]$ genom $N(a + ib\sqrt{3}) = a^2 + 3b^2$.

a) Visa att $N(x,y) = N(x)N(y)$ då $x,y \in Z[\sqrt{-3}]$.

forts.

RB 32 b) Bestäm de invertibla elementen i $Z[\sqrt{-3}]$.

c) Ge exempel på ett primelement i $Z[\sqrt{-3}]$.

d) Är $(2,1 + \sqrt{-3})$ ett principalideal?

e) Är $Z[\sqrt{-3}]$ Euklidisk?

RB 33 Låt $R = \{a + b\sqrt{D}: a,b \in Z$, D fixt heltal som ej är kvadrat av ett heltal$\}$. R är en delring av de reella talen. Visa att $a + b\sqrt{D}$ är invertibelt om och endast om $|a^2 - b^2D| = 1$.

RB 34 a) Bestäm minst sex invertibla element i $Z[\sqrt{17}] = \{a + b\sqrt{17}: a,b \in Z\}$.

b) Visa att $9 - 2\sqrt{17}$ är primelement i $Z[\sqrt{17}]$.

c) Visa att $-11 + \sqrt{17}$ ej är primelement i $Z[\sqrt{17}]$.

d) Uppdela 8 på olika sätt i primfaktorer i $Z[\sqrt{17}]$.

e) Är $Z[\sqrt{17}]$ en Euklidisk ring?

RB 35 Visa att ringen P i RA 17 g är isomorf med $Z[i]$.

RB 36 Primfaktoruppdela i $Z_3[X]$

a) $X^4 + \bar{2}X^3 + X^2 + X + \bar{1}$

b) $X^4 + \bar{2}X^3 + \bar{2}X + \bar{2}$

RB 37 Primfaktoruppdela i $Z_5[X]$

a) $X^4 + \bar{2}X^3 + X^2 + \bar{1}$

b) $X^4 + \bar{4}X^3 + X^2 + \bar{4}X + \bar{2}$

RB 38 a) Bestäm största gemensamma delare till $f(X) = X^3 - \bar{2}X^2 + \bar{2}X + \bar{5}$ och $g(X) = X^3 + \bar{4}X + \bar{2}$ i $Z_{11}[X]$ och skriv den på formen $s(X)f(X) + t(X)g(X)$ med $s(X), t(X) \in Z_{11}[X]$.

b) Samma uppgift för $f(X) = X^3 + X^2 + \bar{5}X + \bar{5}$ och $g(X) = X^3 + \bar{2}X^2 + \bar{6}X + \bar{5}$ i $Z_7[X]$.

RB 39 Visa att det finns precis två irreducibla tredjegradspolynom i $Z_2[X]$ och att dessa är faktorer i $X^7 + \bar{1}$.

RB 40 a) Visa att $Z_{13}[X]/(X^2 + \bar{5})$ är en kropp.

b) Hur många element har denna kropp?

c) Vilken är karaktäristiken?

d) Bestäm inversen till det element som representeras av $X^4 + \bar{3}X^2 + X + \bar{3}$.

RB 41 a) Visa att $Z_7[X]/(X^3 + \bar{2}X + \bar{1})$ är en kropp.

b) Hur många element har denna kropp?

c) Vilken är karaktäristiken?

d) Bestäm inversen till det element som representeras av $X^2 + \bar{3}$.

RB 42 a) Bestäm antalet nolldelare i $Z_5[X]/(X^2 + \bar{3}X + \bar{2})$.

b) Bestäm antalet nolldelare i $Z_3[X]/(X^3 + X^2 + \bar{2}X + \bar{2})$.

RB 43 a) Ange alla ideal i $R = Z_5[X]/(X^2 + \bar{3}X + \bar{2})$.

b) Ange alla ideal i $S = Z_3[X]/(X^3 + X^2 + \bar{2}X + \bar{2})$.

RB 44 Avgör om följande par av ringar är isomorfa

a) $Z_3[X]/(X + \bar{1})$ och $Z_3[X]/(X - \bar{1})$

b) $Z_3[X]/(X^2 + \bar{1})$ och $Z_3[X]/(X^2 - \bar{1})$.

RB 45 Visa att det ideal i $Q[X]$ som genereras av $X^4 + X^3 + 3X^2 + X + 2$ och $X^3 + X^2 + 5X + 3$ är hela $Q[X]$.

RB 46 Undersök om det ideal i $Q[X]$ som genereras av $2X^4 + 2X^3 + 3X^2 + X + 1$ och $6X^3 - 4X^2 + 3X - 2$ är maximalt.

RB 47 a) Visa att $Q[X]/(X^2 + X + 1)$ är en kropp.

b) Låt A vara mängden av alla ordnade par (a,b) av rationella tal med $(a,b) + (c,d) = (a + c, b + d)$ och $(a,b)(c,d) = (ac - bd, ad + bc - bd)$. Visa att A är en kropp t.ex. genom att visa att den är isomorf med kroppen i a).

RB 48 Visa att $X^5 - X^2 + 1$ är irreducibelt i $Q[X]$ genom att betrakta motsvarande polynom i $Z_2[X]$.

RB 49 Visa att $X^4 + 3X^3 + 3X^2 - 5$ är irreducibelt i $Q[X]$ genom att betrakta motsvarande polynom först i $Z_2[X]$ sedan i $Z_3[X]$.

RB 50 a) Visa att mängden av polynom i $Q[X]$ som saknar X-term bildar en delring av $Q[X]$.

b) Visa att X^2 och X^3 är primelement i denna ring.

c) Har ringen entydig faktorisering?

RB 51 $a \in Q$. Visa att $\{f(X) \in Q[X];\ f(a) = 0\}$ är ett maximalideal M i $Q[X]$ och att $Q[X]/M$ är isomorf med Q.

RB 52 Ange ett maximalideal som omfattar $(X^2 + 2)$ i

a) $C[X]$

b) $Q[X]$

c) $Z[X]$.

RB 53 I ringen $Z[X]$ betraktas idealet $A = (X - 2, 2X - 1)$. Visa att $A \neq Z[X]$.

RB 54 Visa att det enda ideal i $Z[X]$, som innehåller polynomen $X^3 + 4X^2 + 3X$ och $X^2 + 3X + 1$ är $Z[X]$ själv.

RB 55 Visa att $Z[X,Y]$ inte är en euklidisk ring.

RB 56 Visa att $Q[X,Y]/(X,Y - 1)$ är isomorf med Q.

RB 57 I $Z[X,Y]$ betraktas idealet $A = (X - 3, X + 2)$

a) Visa att $A \neq Z[X]$.

b) Hur många element har $Z[X]/A$?

RB 58 Bestäm alla maximalideal i $Z[X]$ som omfattar idealet $(6,X^2)$.

Uppgifter

RC 1 R är en kommutativ ring med etta sådan att $a^2 = 1$ för alla $a \neq 0$ i ringen. Visa att antingen är $2a = 0$ för alla $a \in R$ eller är $3a = 0$ för alla $a \in R$. Bestäm alla sådana ringar.

RC 2 a och b är element i en kommutativ ring. a är invertibelt och b är nilpotent (d.v.s. $b^n = 0$ för något n). Visa att a + b är invertibelt.

RC 3 Ett element u i en ring med etta har en högerinvers, d.v.s. det finns ett element u_1 så att $uu_1 = 1$.

a) Visa att följande tre påståenden är ekvivalenta:

i) u har fler högerinverser

ii) u är ej invertibelt

iii) u är vänsternolldelare, d.v.s. det finns ett element $v \neq 0$ så att $uv = 0$.

b) Visa att i en ändlig ring kan ett element inte ha mer än en högerinvers.

RC 4 Låt A vara en kommutativ ring med p element, p primtal och sådan att det finns produkter $\neq 0$ i A. Visa att A är isomorf med Z_p.

RC 5 Bestäm alla ringar med eller utan etta som har tre element.

RC 6 A är en kommutativ ring utan nolldelare, sådan att varje additiv delgrupp till A är ett ideal. Bestäm alla sådana A.

RC 7 Låt $A = \{\begin{pmatrix} x & 0 \\ y & x \end{pmatrix}: x,y \in R\}$.

a) Visa att A är en kommutativ delring av ringen av 2X2-matriser med reella tal som koefficienter.

b) Bestäm alla ideal i A.

RC 8 Bestäm alla ideal i, och homomorfa bilder av $\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}: a,b,c \in Q\}$.

RC 9 Låt R vara ringen av matriser $\begin{pmatrix} a & 0 \\ b & a \end{pmatrix}$ där $a,b \in Z$. Bestäm alla integritetsområden, som är homomorfa bilder av R.

RC 10 Bestäm alla ideal i ringen av 2X2-matriser med koefficienter i

a) Q

b) Z

RC 11 I en kommutativ ring med enhetselement är I ett ideal, som ej innehåller något strikt mindre ideal utom nollidealet. Visa att antingen är produkten av två element i I alltid 0 eller också finns det ett element i I som fungerar som enhetselement för ringen I.

RC 12 Låt R och S vara ringar och f en avbildning från R till S sådan att

i) för varje $a,b \in R$ gäller $f(a + b) = f(a) + f(b)$

ii) för varje fixt par $a,b \in R$ gäller $f(ab) = f(a)f(b)$ eller $f(ab) = f(b)f(a)$.

Visa att antingen gäller $f(ab) = f(a)f(b)$ för <u>alla</u> $a,b \in R$, eller också gäller $f(ab) = f(b)f(a)$ för <u>alla</u> $a,b \in R$.

RC 13 På mängden R^2 av reella talpar definieras addition och multiplikation genom $(x_1,y_1) + (x_2,y_2) = (x_1 + x_2, y_1 + y_2)$ och $(x_1,y_1) \cdot (x_2,y_2) = (x_1x_2 + y_1y_2, x_1y_2 + x_2y_1)$. Visa att härigenom blir R^2 en kommutativ ring med etta samt bestäm alla ideal i denna ring.

RC 14 En ring kallas Boolesk om $x^2 = x$ för varje $x \in R$.

a) Visa att ringen i RA 16 är Boolesk.

b) Visa att en Boolesk ring är kommutativ och att $x + x = 0$ för varje $x \in R$.

c) Visa att en Boolesk ring utan nolldelare antingen är 0 eller isomorf med Z/(2).

RC 15 Låt R beteckna mängden av konvergenta reella talföljder $(x_n)_1^\infty$. R blir en ring om man definierar

$(x_n) + (y_n) = (x_n + y_n)$ och

$(x_n)(y_n) = (x_n y_n)$

a) Visa att $I = \{(x_n)\colon \lim x_n = 0\}$ är ett ideal i R.

b) Visa att I är ett maximalideal.

RC 16 Bilda ringen Z⊕Z enligt RA 9.

a) Ange de invertibla elementen i Z⊕Z.

b) Undersök om något av följande element genererar ett maximalideal i Z⊕Z: (p,q), (1,pq), (p,1), (1,0), **p,q primtal.**

c) Visa att varje ideal i R är principalt.

RC 17 Låt A vara mängden av reellvärda funktioner definierade på hela reella axeln. A är kommutativ ring om addition och multiplikation definieras genom $(f + g)/(x) = f(x) + g(x)$ resp. $(fg)(x) = f(x) \cdot g(x)$. Visa att om M är en mängd av reella tal så är $I_M = \{f \in A \mid f(x) = 0 \text{ då } x \in M\}$ ett ideal i A. För vilka M är I_M maximalideal?

RC 18 K är en kommutativ kropp, A är en delring till K. A kallas valuationsring om $A \neq K$ och för varje $x \in K$ gäller $x \in A$ eller $x^{-1} \in A$. Visa att mängden av icke-invertibla element bildar ett maximalt ideal i A.

RC 19 A är en kommutativ ring med etta där varje element x satisfierar $x^n = x$ för något $n > 1$. Visa att om P är ett ideal sådant att A/P är ett integritetsområde, så är P ett maximalideal.

RC 20 Ett ideal I i en ring kallas minimalt om $I \neq (0)$ och I ej innehåller några andra ideal än I och (0). Visa att om det i en euklidisk ring R finns ett minimalt ideal så måste R vara en kropp.

RC 21 Ge exempel på ett element r, som inte har entydig faktoruppdelning, i en ring R sådan att

a) R har nolldelare

b) R har inga nolldelare och saknar etta

c) R har inga nolldelare och har etta.

RC 22 Bestäm samtliga ringhomomorfa avbildningar av $Z[i]$ på Z_5.

RC 23 I ekvationen $aX^2 + bX + c$ är a,b,c udda hela tal. Visa att ekvationen saknar rationella rötter.

RC 24 $R = Z_3[X]/(X^4 + \bar{1})$.

a) Hur många element har R?

b) Visa att $3a = 0$ och $a^9 = a$ gäller för varje $a \in R$.

c) Låt M vara ett maximalideal i R och låt y vara bilden av X under den sammansatta avbildningen $Z_3[X] \to R \to R/M$. Visa att R/M är en kropp med de 9 elementen $0,1,y,\ldots,y^7$.

RC 25 Uppdela polynomet $X^4 + X^3 + \bar{3}X^2 + \bar{2}$ i ringen $Z_5[X]$ i irreducibla faktorer. Ange alla ideal i ringen $R = Z_5[X]/(X^4 + X^3 + \bar{3}X^2 + \bar{2})$. Hur många invertibla element finns det i R?

RC 26 a) Visa att $XY + Y + 1$ och $XY - X$ är relativt prima i $Q[X,Y]$ (saknar gemensamma primfaktorer i $Q[X,Y]$).

b) Visa att $(XY + Y + 1, XY - X) \neq Q[X,Y]$.

RC 27 Gäller satsen om entydig faktoruppdelning i ringen $Z[X,Y]/(2,X^3 + X + 1)$?

Svar

RA 1 a), d) och e) är ringar.

RA 2 I d) och e) är $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ etta, a) saknar etta.

a) är kommutativ.

I a) är 0 nollelement, i d) och e) är $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ nollelement.

RA 4 Ettan är den funktion som är identiskt 1. Nollelement är den funktion som är identiskt noll. Låt $f(x) = \begin{cases} 0, & x \neq 0 \\ 1, & x = 0 \end{cases}$

Då är $f(x) \cdot x$ identiskt noll. De funktioner $g(x)$, som har något nollställe, är nolldelare.

RA 5 a) a

b) Alla element är sina egna additiva inverser.

c) Nej

d) Nej

e) Ja; **b, c, d är nolldelare.**

f) Ja

g) Nej

RA 6 b) Om inverserna till a resp. b är a^{-1} resp. b^{-1} så har ab inversen $b^{-1}a^{-1}$.

RA 7 Om a har inversen a^{-1} så har -a inversen $-a^{-1}$.

RA 9 b) Nej (utom då A eller B är en nollring).

RA 10 $a^3 + a^2b + ab^2 + b^3 + aba + bab + ba^2 + b^2a$

RA 16 b) Ja

c) Ja, S är ringens etta.

RA 17 b) $(0,0,0,0)$

c) $(-a,-b,-c,-d)$

d) $(1,0,0,1)$ är etta.

e) De element (a,b,c,d) för vilka $ad - bc \neq 0$.

f) Nej

h) Ja

j) Nej

k) Inversen till $(z_1,z_2,-\bar{z}_2,\bar{z}_1)$ är $(\bar{z}_1/r,-z_2/r,-\bar{z}_2/r,z_1/r)$ där $r = |z_1|^2 + |z_2|^2$.

RA 18 b) $(0,0)$

c) Ja, $(0,1)$ är ettan.

RA 19 c) Nej. Tag t.ex. den naturliga homomorfismen av Z på Z_4.

RA 20 a) Ja

b) Nej

RA 21 b) $\{(a,0)\}$

RA 24 b) Nej

RA 26 a) Ja

b) Nej

c) Nej

RA 27 c) $\{(0,0,c,0)\}$

d) Nej

RA 28 c) Ja

d) RXZ/RX{0} är isomorf med Z.

RA 29 a) 13

b) $13 = 3 \cdot 156 - 5 \cdot 91$

RA 31 a) Ja

b) Ja

c) Nej

RA 32 a) Ja

b) Nej

RA 35 3Z

RA 36 3Z

RA 37 2Z

RA 38 b delar a.

RA 39 a) $A \subseteq B$ eller $B \subseteq A$.

b) Alltid

RA 40 De additiva delgrupperna till G.

RA 44 c) d = 2

d) d = (m,n) d.v.s. största gemensamma delare till m och n.

RA 45 d) d = 24

e) d = 12

f) d = mn

g) d = mn/(m,n), d.v.s. minsta gemensamma multipel av m och n.

RA 46 d) d = 2

e) d = 4

f) d = m/(m,n) = produkten av de primfaktorer (med potenser) som ingår i m men fattas i n. (Om t.ex. $m = 72 = 2^3 \cdot 3^2$ och $n = 10 = 2 \cdot 5$ är $d = 36 = 2^2 \cdot 3^2$.)

RA 47 d) $d = 2$

e) $d = 6$

f) Om $m = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$ med $n_i > 0$ och p_i olika primtal så är $d = p_1 p_2 \cdots p_k$.

RA 48 a) Nej

b) Nej

RA 49 e) $\{ra + na: r \in R, n \in Z\}$ om R är kommutativ, $\{r_1 a + a r_2 + na : r_1, r_2 \in R, n \in Z\}$ om R är ickekommutativ. (Om R har etta behöver man inte ta med termerna na i ovanstående uttryck.)

RA 50 d) {a,b} är ett högerideal, men inte vänsterideal och därmed inte heller ett ideal.

RA 51 Endast högerideal.

RA 52 b) Alla pZ, p primtal.

d) T.ex. maximalidealet $4Z$ i ringen $2Z$.

RA 55 a) Summan = $\bar{3}X$, produkten = $X^4 + \bar{2}X^3 + X^2 + \bar{4}X + \bar{4}$

b) Summan = $X^4 + X^3 + X^2$, produkten = $X^7 + X + \bar{2}$

RA 56

+	$\bar{0}$	$\bar{1}$	X	$X+\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	X	$X+\bar{1}$
$\bar{1}$	$\bar{1}$	0	$X+\bar{1}$	X
X	X	$X+1$	$\bar{0}$	$\bar{1}$
$X+\bar{1}$	$X+\bar{1}$	X	$\bar{1}$	$\bar{0}$

·	$\bar{0}$	$\bar{1}$	X	$X+\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	X	$X+\bar{1}$
X	$\bar{0}$	X	$X+\bar{1}$	$\bar{1}$
$X+\bar{1}$	$\bar{0}$	$X+\bar{1}$	$\bar{1}$	X

RA 57 a) $(X^3 + 3X^2 + 3X + 2, X^3 + 2X^2 + X + 2) = X + 2$ och

$X + 2 = (X + 1)(X^3 + 2X^2 + X + 2) - X(X^3 + 3X^2 + 3X + 2)$

b) $(X^3 + X, X^3 + X^2 + X + \bar{1}) = X^2 + \bar{1}$ och

$X^2 + \bar{1} = (X^3 + X^2 + X + \bar{1}) - (X^3 + X)$

RA 58 $X,\ X + \bar{1},\ X^2 + X + \bar{1},\ X^3 + X^2 + \bar{1},\ X^3 + X + \bar{1}$

RA 59 $(p^2 - p)/2$

RA 61 a) $(X + \bar{1})(X^3 + X + \bar{1})$

b) $(X^2 + X + \bar{1})^2$

c) $(X + 4)(X^3 + X^2 + X + 3)$

d) $\bar{4}(X + \bar{1})(X + \bar{3})^2(X + \bar{6})$

RA 64 a) $(X - 1)(X + 1)(X^2 + 1)$ i $Q[X]$ och $R[X]$, $(X - 1)(X + 1)(X + i)(X - i)$ i $C[X]$.

b) $(X - 1)(2X + 1)(2X + 3)(X^2 - 2)$ i $Q[X]$,

$(X - 1)(2X + 1)(2X + 3)(X - \sqrt{2})(X + \sqrt{2})$ i $R[X]$ och $C[X]$.

Svar

RB 1 b) Isomorf med Z.

c) Isomorf med Z_n, där n är ordningen av gruppen.

d) Isomorf med Q.

RB 2 a) Nej.

b) Ja.

RB 3 a) bc = c, bd = d, cb = a, cc = a, dd = d.

b) Nej

c) Nej

RB 4 a) aa = ab = ac = ad = a, bc = a, bd = b, cb = a, cc = c, dd = d.

b) Ja

c) Ja, d är etta.

RB 6 $\{m \in Z_n: (m,n) = 1\}$

RB 9 Z_{pq}, Z_p, Z_q, nollringen.

RB 10 a) Z, nollringen.

b) Q, nollringen.

RB 11 e) $\{a/b \in R: (a,p) = 1\}$.

f) $\{p^n R: n \geq 0\}$.

RB 13 $a = p^2$, p primtal.

RB 14 b) Kropparna är isomorfa.

RB 17 b) Ja.

RB 20 pR är det enda maximala idealet.

RB 21 b) p är det enda primelementet (bortsett från associerade).

RB 22 a) Alla tal $4k + 2$, $k \in Z$.

b) Nej

RB 23 a) $(1 + 2i)(3i + 2)$

b) Primtal

c) $(1 + 2i)(5 + 2i)(3 - 2i)$

d) Primtal

e) $(7 + 2i)(7 - 2i)$

RB 24 a) $2 - i = (1+i)(6 + 2i) - i(9 - 2i)$

b) $1 = (1 + i)(2 - i) - (2 + i)$

c) $2 + i = (7 + i) - 5$

RB 25 a) $(2 - i)Z[i]$

b) $Z[i]$

c) $(2 + i)Z[i]$

RB 26 a) $(22 + 14i)Z[i]$

b) $5 \cdot Z[i]$

c) $(15 - 5i)Z[i]$

RB 27 b) 5

c) 5

d) Den restklass som representeras av $1 + i$.

RB 28 b) 3

c) 9

d) Den restklass som representeras av i.

RB 29 b) Den restklass som representeras av $3 + 3i$.

RB 30 a) $(1 + i)\mathbb{Z}[i]$

b) $(2 + i)\mathbb{Z}[i]$ eller $(2 - i)\mathbb{Z}[i]$.

RB 31 b) 1 och -1.

c) T.ex. $1 + \sqrt{-2}$

RB 32 b) 1 och -1.

c) T.ex. $\sqrt{-3}$.

d) Nej.

e) Nej.

RB 34 a) $1, -1, 4 + \sqrt{17}, 4 - \sqrt{17}, -4 + \sqrt{17}, -4 - \sqrt{17}$.

d) $2 \cdot 2 \cdot 2 = (3 + \sqrt{17})(\sqrt{17} - 3) = (5 + \sqrt{17})(5 - \sqrt{17})$ är olika uppdelningar.

e) Nej.

RB 36 a) $(X + \bar{1})(X + \bar{2})(X^2 + \bar{2}X + \bar{2})$

b) $(X^2 + \bar{1})(X^2 + \bar{2}X + \bar{2})$

RB 37 a) $(X + \bar{4})(X + \bar{2})(X^2 + X + \bar{2})$

b) $(X^2 + \bar{2}X + \bar{3})(X^2 + \bar{2}X + \bar{4})$

RB 38 a) $\bar{1} = (\bar{6}X^2 + \bar{7}X + \bar{8})(X^3 + \bar{4}X + \bar{2}) - (\bar{6}X^2 + \bar{8}X + \bar{3})(X^3 - \bar{2}X^2 + \bar{2}X + \bar{5})$

b) $X + \bar{1} = (\bar{3}X + \bar{3})(X^3 + X^2 + \bar{5}X + \bar{5}) - \bar{3}X(X^3 + \bar{2}X^2 + \bar{6}X + \bar{5})$

RB 40 b) 169

c) 13

d) Det element som representeras av $\bar{5}X$.

RB 41 b) 7^3

c) 7

d) Det element som representeras av $\bar{5}X^2 + \bar{5}X + \bar{2}$.

RB 42 a) 8

b) ~~14~~ 15

RB 43 a) R,$(X + 1)$R, $(X + 2)$R och nollidealet i R.

b) S, $(X + 1)$S, $(X + 2)$S, $((X + 1)^2)$S, $((X + 1)(X + 2))$S och nollidealet i S.

RB 44 a) Isomorfa

b) Icke-isomorfa

RB 46 Ja, $(2X^2 + 1)\mathbb{Q}[X]$ är maximalt.

RB 50 c) Nej

RB 52 a) $(X + i\sqrt{2})\mathbb{C}[X]$

b) $(X^2 + 2)\mathbb{Q}[X]$

c) $(2,X)$

RB 57 b) 5

RB 58 $(2,X)$ och $(3,X)$.

Svar

RC 1 Z_2, Z_3 och nollringen.

RC 5 Z_3 och den ring som består av elementen a, 2a och 0, med 3a = 0 och $a^2 = 0$ (och därmed alla produkter = 0).

RC 6 Antingen är A isomorf med nZ något $n \geq 0$, eller också är A isomorf med Z_p, p primtal.

RC 7 b) Hela ringen, $\{\begin{pmatrix} 0 & 0 \\ y & 0 \end{pmatrix}\}$ och nollidealet.

RC 8 Nollidealet, $\{\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}: b \in Q\}$, $\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}: a,b \in R\}$, $\{\begin{pmatrix} 0 & b \\ 0 & c \end{pmatrix}: b,c \in R\}$ samt hela ringen är idealen i ringen.

Homomorfa bilder är isomorfa med någon av följande ringar:
hela ringen, $\{\begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix}: a,c \in R\}$ (som är isomorf med $Q \oplus Q$),
$\{\begin{pmatrix} 0 & 0 \\ 0 & c \end{pmatrix}: c \in R\}$ (som är isomorf med Q), $\{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}: a \in R\}$ (som är isomorf med Q) samt nollringen.

RC 9 De ringar som är isomorfa med Z eller Z_p, p primtal.

RC 10 a) Nollidealet och hela ringen.

b) Nollidealet samt I_n = {matriser där varje koefficient är delbar med n}, för n = 1,2,...

RC 13 Idealen blir (förutom nollidealet och hela ringen):
$((-1,1))R^2$ och $((1,1))R^2$.

RC 16 a) De invertibla elementen är: (1,1), (1,-1), (-1,1) och (-1,-1).

b) Endast (p,1) genererar ett maximalideal.

RC 17 De mängder som består av en punkt.

RC 21 a) I $Z_4[X]$ är $X^2 = X \cdot X = (X - \bar{2})(X - \bar{2})$.

b) I $2Z$ är $36 = 6 \cdot 6 = 2 \cdot 18$.

c) I $Z[\sqrt{-5}] = \{a + b\sqrt{-5}\}$ är $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

RC 22 De avbildningar som ges av $f(a + ib) = \overline{a + 2b}$ och $g(a + ib) = \overline{a + 3b}$.

RC 24 a) 81

RC 25 Idealen är: nollidealet, $(X + \bar{1})R$, $(X^3 - \bar{2}X + \bar{2})R$ samt R. Antalet invertibla element är 496.

RC 27 Ja.

Ledningar

RA 3 Det räcker att visa att mängden är sluten under subtraktion (se anm. efter lösningen) och multiplikation, d.v.s. att dessa operationer inte leder utanför mängden. Räknereglerna är automatiskt uppfyllda, eftersom mängden är en delmängd av de reella talen som uppfyller alla räkneregler för en ring.

RA 5 c) Om e är etta ska gälla re = r och er = 4 för varje r M.

d) Är multiplikationstabellen symmetrisk?

f) och g) Det räcker att undersöka om delmängderna är slutna under subtraktion (bildar delgrupp under addition, se anm. efter lösningen av RA 3) och multiplikation.

RA 9 b) Antag $a \in A$, $a \neq 0$ och $b \in B$, $b \neq 0$. Multiplicera (a,0) med (0,b).

RA 11 $[x,[y,z]] = [x,yz - zy] = x(yz - zy) - (yz - zy)x = xyz - xzy - yzx + zyx.$

RA 13 Visa att a(-b) och (-b)a båda är lika med -ab, d.v.s. att de båda är additiva inverser till ab.

RA 17 e) Observera att en invers är både vänster- och högerinvers. Räkningarna blir något mödosamma.

RA 20 a) Visa att $f(a + b\sqrt{3}) = a + b\sqrt{2}$ är en gruppisomorfism.

b) $f(1) = 1$ (se RA 19) ger $f(2) = f(1 + 1) = f(1) + f(1) = 1 + 1 = 2$ för en ringisomorfism, men $f(2) = f(\sqrt{2}\cdot\sqrt{2}) = f(\sqrt{2})f(\sqrt{2})$. Slutsats?

RA 24 b) $f(\begin{pmatrix} 0 & 0 \\ 0 & b \end{pmatrix}) = 0$ för varje b.

RA 26 b) $f(0,b-b,0) = 0$ för varje b.

RA 30 a) Se lösningen av RA 29 b.

b) Antag att a och b har en gemensam primtalsfaktor p.

Vad kan man då säga om ma + nb?

RA 32 Se lösningen av RA 31.

RA 33 $(24,52) = 4$. Jämför RA 29 b.

RA 35 Se lösningen av RA 34.

RA 37 Se lösningen av RA 36.

RA 38 Speciellt gäller $a \in bZ$. Använd detta.

RA 39 Se svaret och försök sedan lösa uppgiften.

RA 40 Betrakta en godtycklig additiv delgrupp. När är den ett ideal?

RA 44 c) och d) Jämför RA 34.

RA 45 c) Visa alltså att $AB \subseteq A$ och att $AB \subseteq B$.

e) Vilka tal är multipler både av 4 och 6?

RA 48 a) $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ a & b \end{pmatrix}$

b) $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}$

RA 49 b) Jämför RA 48 b.

c) Man ska visa: i) $a \in aR$ ii) Varje ideal som innehåller a omfattar hela aR.

d) Betrakta $R = 2Z$, $a = 2$.

RA 53 Använd att $a \in bR$ d.v.s. $a = br$ och att $b \in aR$ d.v.s. $b = as$.

RA 59 Hur många andragradspolynom med högstagradskoefficient 1 finns totalt? Hur många av dessa är reducibla?

RA 60 $\bar{3}$ är invertibelt.

RA 64 b) Vilka rationella nollställen kan finnas?

RA 65 a) Låt $f(X)$, $g(X)$ vara $\neq 0$. Betrakta högstagradstermen i $f(X)g(X)$.

b) Kan ett polynom av grad ≥ 1 ha invers?

RA 66 b) Vad är $(bj + ck + dl)^2$?

Ledningar

RB 1 b)c) En endomorfism av en cyklisk grupp är bestämd av bilden av en generator och denna bild kan vara vilket element som helst.

d) Visa att det räcker att känna bilden av 1 för att känna hela endomorfismen och att bilden av 1 kan vara vilket element som helst.

RB 2 a) Låt y vara en inverterbar idempotent. Multiplicera $y^2 = y$ med y^{-1}.

b) Betrakta t.ex. Z_6.

RB 3 cb = (d + b)b o.s.v.

RB 4 Vilket element är nollelement? Jfr sedan RB 3.

RB 7 a) Låt $a^n = 0$. Beräkna $\sum_{n=1}^{\infty} a^n$ och multiplicera med 1-a.

RB 8 Man ska visa: Om C är ett ideal sådant att A/C är kommutativ, så innehåller C det i uppgiften beskrivna idealet.

RB 9 Vilka ideal finns i Z_{pq}? (Vilka ideal finns i Z som omfattar pqZ?)

RB 10 Vilka möjliga bilder av ettan finns?

RB 13 Idealen i Z_a svarar mot idealen i Z som omfattar aZ.

RB 14 b) Vilket element är etta i 2)? Vid en isomorfism måste ettan i 1) avbildas på ettan i 2). Detta bestämmer hela avbildningen. Visa att denna avbildning verkligen blir en isomorfism.

RB 15 b) Låt t.ex. $f(\begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{0} \end{pmatrix}) = b$ och $f(\begin{pmatrix} \bar{0} & \bar{0} \\ \bar{1} & \bar{0} \end{pmatrix}) = c$. Utvidga denna avbildning på det enda möjliga sättet, och visa att det blir en isomorfism.

RB 16 a) $h(mn) = h(\underbrace{1 + 1 + \ldots + 1}_{mn \text{ element}}) = \underbrace{h(1) + h(1) + \ldots + h(1)}_{mn \text{ element}}$

RB 17 a) Vilket element måste vara etta i $(Z,*,o)$?

Bestäm med ledning därav isomorfismen (samtidigt visas att $(Z,*,o)$ är en ring).

RB 18 Låt n vara ordningen av ringens etta. Visa att $na = 0$ för varje $a \in R$. Då måste ettan vara generator för den additiva gruppen. (Varför?)

RB 19 Visa att R/M är isomorf med Q.

RB 21 a)b) Varje element kan skrivas $p^n u$, $n \geq 0$, u invertibel. Betrakta $d(p^n u) = n$.

RB 22 b) En Euklidisk ring har speciellt etta.

RB 23 Använd att $N(z_1 z_2) = N(z_1)N(z_2)$ om $N(a + ib) = a^2 + b^2$.

RB 28 Jfr lösningen av RB 27.

RB 29 a) Är $5 + 12i$ ett primtal?

b) Använd Euklides algoritm.

RB 30 Alla ideal i $Z[i]$ är principala. Vilka element genererar maximalideal?

RB 32 a)b)c) Jfr lösningen av RB 31.

e) I en Euklidisk ring är varje ideal principalt.

RB 33 Jfr lösningen av RB 31 b.

RB 34 a) Om $N(a + b\sqrt{17}) = a^2 - 17b^2$ gäller $N(xy) = N(x)N(y)$. Ett element är invertibelt om och endast om $|N(x)| = 1$.

b) Ett element med primtalsnorm är irreducibelt.

c) $N(xy) = N(x)N(y)$.

d) Visa att element med norm 4 eller 8 är irreducibla.

e) I en Euklidisk ring gäller satsen om entydig faktorisering.

RB 40 d) Använd Euklides algoritm.

RB 41 Jfr lösningen av RB 40.

RB 42 b) Jfr lösningen av RB 42 a.

RB 43 b) Jfr lösningen av RB 43 a.

RB 44 b) Finns nolldelare i ringarna?

RB 45 Det ideal som genereras av de två polynomen, är det ideal som genereras av största gemensamma delaren till polynomen.

RB 46 Se ovan. När är $aQ[X]$ maximalt?

RB 47 a) $X^2 + X + 1$ är irreducibelt.

b) Elementen i kroppen kan representeras av förstagradspolynom i $Q[X]$. Betrakta $\overline{a + bX} \to (a,b)$.

RB 48 Om polynomet är reducibelt i $Q[X]$, så är det reducibelt i $Z[X]$. Om det är reducibelt i $Z[X]$, så är motsvarande polynom i $Z_2[X]$ reducibelt.

RB 49 Se ovan.

RB 50 c) Uppdela t.ex. X^6 på olika sätt.

RB 53 Visa att $1 \notin A$, t.ex. genom att visa att $A = (X - 2, 3)$.

RB 54 Visa att 1 kan skrivas som linjärkombination av $X^3 + 4X^2 + 3X$ och $X^2 + 3X + 1$. Använd t.ex. Euklides algoritm.

RB 55 Visa att $Z[X,Y]$ inte är en principalidealring. Betrakta t.ex. idealet (X,Y)

RB 56 Visa först att $Q[X,Y]/(X,Y-1)$ är isomorf med $Q[Y]/(Y - 1)$.

RB 57 a) Visa att $1 \notin A$.

b) Visa t.ex. att $A = (X - 3,5)$.

Ledningar

RC 1 Om varken 1, 1 + 1 eller 1 + 1 + 1 = 0 i R gäller $2 \cdot 2 = 4 \neq 1$. Visa att ringarna nollringen, Z_2 och Z_3 uppfyller kravet. Försök utvidga dessa ringar med ett element med bibehållande av $a^2 = 1$ för varje a. Använd t.ex. likheterna $(a + 1)^2 = 1$, $(a + 1)^3 = 1$.

RC 2 Använd formeln $(a + b)(a^k - a^{k-1}b + a^{k-2}b^2 - \ldots + (-1)^k b^k) = (a^{k+1} - b^{k+1})$.

RC 3 a) Visa att i) medför ii) medför iii) medför i). Observera att förutsättningen "u har en högerinvers" gäller hela tiden.

b) Visa att varje element i ringen (speciellt 1) kan skrivas som $u_1 r$ för något $r \in R$, och att u_1 därmed har en högerinvers. Visa att denna måste vara u, och använd sedan ii) ovan.

RC 4 Ett ideal är speciellt en additiv delgrupp. Ringen har alltså bara de triviala (0) och A. Varför? Låt $a \in A$ vara sådant att $ab \neq 0$ för något $b \in A$. Visa att ringen har en etta genom att betrakta idealet $\{ra \mid r \in A\}$.

RC 5 Undersök först ringar med etta. Visa att här måste 2 = 0 eller 3 = 0. Varför kan man utesluta det första alternativet? Undersök sedan ringar utan etta. Vilka möjligheter finns här till multiplikation?

RC 6 Betrakta den additiva delgrupp, som genereras av ett element $a \neq 0$. Då gäller för varje $r \in A$ att $ra = na$ för något n. Visa att $r \to n$ ger en homomorfism.

RC 7 b) Låt I vara ett ideal $\neq 0$. Om I innehåller en matris med diagonalelement $\neq 0$, så innehåller I också enhetsmatrisen.

RC 8 Jfr lösningen av RC 7.

RC 9 Bestäm alla nolldelare i R. Visa att för en sådan gäller $x^2 = 0$. Alla nolldelare måste alltså ingå i kärnan (varför?). Vilka ideal omfattar alla nolldelare? Vilka av dessa ger upphov till integritetsområden?

RC 10 Jfr lösningen av RC 7.

RC 11 Låt $a \in I$, $a \neq 0$. Då bildar $\{ra \mid r \in \text{ringen}\}$ ett ideal. Antingen är $a^2 = 0$ eller $(a^2) = (a)$.

RC 12 Visa först att $f(0) = 0$, $f(-a) = -f(a)$. Visa sedan genom att studera $f(ab)$, som antas $= f(a)f(b)$, och $f(ac)$, som antas $= f(c)f(a)$, och $f(a(b - c))$, att för ett fixt a gäller antingen $f(ab) = f(a)f(b)$ för alla b eller $f(ab) = f(b)f(a)$ för alla b. Antag sedan $f(ab) = f(a)f(b)$ men ej $= f(b)f(a)$ för alla b, och att $f(cb) = f(b)f(c)$ men ej $= f(c)f(b)$ för alla b. Betrakta $f((a - c)b)$.

RC 13 Visa att den givna ringen blir isomorf med $R[X]/(X^2 - 1)$.

RC 14 b) Betrakta $(x + x)^2$ och $(x + y)^2$.

c) Visa att $xy(x + y) = 0$ för varje x och y.

RC 16 Vilket element blir enhetselement? Använd det faktum att restklassringen modulo ett maximalideal är en kropp. För att visa att varje ideal I är principalt, visa att det finns bland $\{a \mid (a,b) \subseteq I\}$ finns ett minsta element a_o, och att varje $a \in I$ är delbart med a_o, och att motsvarande gäller för $\{b \mid (a,b) \in I\}$, där motsvarande element kallas b_o. Visa att $(a_o, b_o) \in I$.

RC 18 Låt x och y vara icke-invertibla. Att xy är icke-invertibel är lätt att visa. För att visa att $x + y$ är icke-invertibel, antag $x/y \notin A$. $y(1 + x/y) = y + x$.

RC 20 En euklidisk ring är principalidealring. Antag (a) är ett minimalt ideal. Betrakta (a^2).

RC 21 a) Betrakta t.ex. $Z_4[X]$.

b) Betrakta t.ex. $2\mathbb{Z}$.

c) Betrakta t.ex. $Z[\sqrt{-5}]$.

RC 22 Undersök vilka av avbildningarna $f(a + ib) = \bar{a} + k\bar{b}$, $k = \bar{0},\bar{1},\bar{2},\bar{3},\bar{4}$ som verkligen blir ringhomomorfismer.

RC 24 Använd att alla element i R kan representeras av polynom av grad ≤ 3 i $Z[X]$. (Hur många element har då R?) $3a = 0$ följer av att $\bar{3} = \bar{0}$ i Z_3. Likheten $a^9 = 0$ kan visas på följande sätt: Visa den först för elementen i Z_3 och sedan för den restklass $\bar{X}$ som bestäms av X och därmed för $\overline{X^2}$ och $\overline{X^3}$. Använd att varje element i R kan skrivas som $a_o + a_1\bar{X} + a_2\overline{X^2} + a_3\overline{X^3}$, där $a_i \in Z_3$, och att $\bar{3} = \bar{0}$. Faktorisera därefter $X^4 + \bar{1}$ i två irreducibla andragradspolynom och visa att ett maximalideal måste innehålla ett av dessa andragradspolynom. Visa att principalidealen, som bestäms av dessa andragradspolynom verkligen blir maximalideal.

RC 25 Undersök eventuella nollställen i Z_5 till $X^4 + X^3 + \bar{3}X^2 + \bar{2}$. Polynomet $p(X)$ i $Z_5[X]$ representerar ett invertibelt element om och endast om $(p(X), X^4 + X^3 + \bar{3}X^2 + \bar{2}) = 1$ i $Z_5[X]$. Visa detta! Använd faktoriseringen för att beräkna antalet invertibla element. $Z_5[X]$ är principalidealring (varför?). Använd faktoriseringen av $X^4 + X^3 + \bar{3}X^2 + \bar{2}$ för att bestämma representanter för generatorerna av idealen i R.

RC 26 b) Antag $P_1(X,Y) \cdot (XY + Y + 1) + P_2(X,Y) \cdot (XY - X) = 1$. Sätt $X = 0$ och $Y = -1$.

RC 27 Visa att $Z[X,Y]/(2, X^3 + X + 1)$ är isomorf med $(Z_2[X]/(X^3 + X + \bar{1}))[Y]$ och att $Z_2[X]/(X^3 + X + \bar{1})$ är en kropp.

Lösningar

RA 3 $a + b\sqrt[3]{3} + c\sqrt[3]{9} - (d + e\sqrt[3]{3} + f\sqrt[3]{9}) = (a - d) + (b - e)\sqrt[3]{3} + (c - f)\sqrt[3]{9}$.

Mängden är sluten under subtraktion och alltså en additiv delgrupp (se anm.) till de reella talen. $(a + b\sqrt[3]{3} + c\sqrt[3]{9})(d + e\sqrt[3]{3} + f\sqrt[3]{9}) =$

$= (ad + 3bf + 3ce) + (ae + bd + 3cf)\sqrt[3]{3} + (af + be + cd)\sqrt[3]{9}$. Mängden är sluten under multiplikation och är alltså en ring, eftersom räknelagarna är uppfyllda (mängden är ju en delmängd av de reella talen).

Anm. Om en delmängd M av en additiv grupp är sluten under subtraktion så är den en delgrupp. Bevis: Om $a \in M$ gäller $a - a = 0 \in M$ och därmed $0 - a = -a \in M$. Om $a,b \in M$ gäller $-b \in M$ enligt ovan, och därmed $a - (-b) = a + b \in M$. M är alltså sluten under inversbildning ($a \in M$ medför $-a \in M$) och addition ($a,b \in M$ medför $a + b \in M$). Detta visar att M är en delgrupp.

RA 6 a) Låt a ha inversen a^{-1}. Multiplikation av $ab = 0$ med a^{-1} från vänster ger $b = 0$, så om $ab = 0$ måste $b = 0$ d.v.s. a är inte nolldelare.

b) Låt a resp. b ha inverserna a^{-1} resp. b^{-1}. Då är $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a \cdot 1 \cdot a^{-1} = aa^{-1} = 1$ och analogt $(b^{-1}a^{-1})(ab) = 1$. ab har alltså inversen $b^{-1}a^{-1}$.

c) Om a och b har inverser så har ab enligt ovan. Om a har invers a^{-1} gäller $aa^{-1} = 1$ och $a^{-1}a = 1$ vilket visar att a^{-1} har inversen a. Enhetselement i gruppen är ringens etta. Associativiteten följer av motsvarande regel för ringmultiplikation.

RA 13 $ab + a(-b) = a(b + (-b)) = a \cdot 0 = 0$,

$ab + (-b)a = ba + (-b)a = (b + (-b))a = 0 \cdot a = 0$. $a(-b)$ och $(-b)a$ är alltså båda additiva inverser till ab och alltså lika.

RA 14 $\begin{pmatrix} a & 2b \\ 0 & a \end{pmatrix} - \begin{pmatrix} c & 2d \\ 0 & c \end{pmatrix} = \begin{pmatrix} a-c & 2(b-d) \\ 0 & a-c \end{pmatrix}$ Mängden är alltså sluten under subtraktion och bildar därmed en additiv grupp. (Se anm. efter lösningen till RA 3.)

$\begin{pmatrix} a & 2b \\ 0 & a \end{pmatrix}\begin{pmatrix} c & 2d \\ 0 & c \end{pmatrix} = \begin{pmatrix} ac & 2(ad+bc) \\ 0 & ac \end{pmatrix}$ Mängden är alltså sluten under multiplikation för diagonalelementen är lika stora hela tal och elementet i övre högra hörnet är ett jämnt heltal. Alla räknelagar följer av att motsvarande lagar gäller för hela matrisringen.

RA 16 $(A \cup B) \setminus (A \cap B) = (B \cup A) \setminus (B \cap A)$ så $A + B = B + A$.

$A + \emptyset = (A \cup \emptyset) \setminus (A \cap \emptyset) = A \setminus \emptyset = A$ för varje $A \in R$. $\emptyset$ är alltså nollelement.

$A + A = (A \cup A) \setminus (A \cap A) = A \setminus A = \emptyset$ för varje $A \in R$. Varje element är alltså sin egen additiva invers.

Vilka mängdelement ingår i $A + (B + C)$, d.v.s. vilken mängd är $A + (B + C)$? $B + C$ består av de mängdelement som finns i B eller C men inte i båda. I $A + (B + C)$ ingår de mängdelement som finns i A eller $(B + C)$ men inte i både A och $(B + C)$, d.v.s. de mängdelement som ligger i precis en av A, B eller C. På samma sätt visas att $(A + B) + C$ är denna mängd. Additionen är alltså associativ.

$A \cap B = B \cap A$ så multiplikationen är kommutativ.

$(A \cap B) \cap C = A \cap (B \cap C)$ så multiplikationen är associativ.

$A(B + C) = A \cap ((B \cap C) \setminus (B \cap C)) = ((A \cap B) \cup (A \cap C)) \setminus (A \cap B \cap C)$

$AB + AC = A \cap B + A \cap C = ((A \cap B) \cup (A \cap C)) \setminus ((A \cap B) \cap (A \cap C)) =$

$= (A \cap B) \cup (A \cap C)) \setminus (A \cap B \cap C)$ så distributiva lagen gäller.

$A \cap S = A$ för varje A, så S är etta i ringen.

RA 19 a) Varje element i S är bild av ett element i R, d.v.s. varje element i S kan skrivas som $f(a)$ för något $a \in R$.

$f(a)f(b) = f(ab) = f(ba) = f(b)f(a)$

b) $f(1)f(a) = f(1 \cdot a) = f(a) = f(a \cdot 1) = f(a)f(1)$ för varje $f(a)$.

c) Se svaret.

RA 22 $f((a + ib) + (c + id)) = f((a + c) + i(b + d)) = \begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix}$

$f(a + ib) + f(c + id) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix}$

$f(a + ib)f(c + id) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix}$

$f((a + ib)(c + id)) = f((ac - bd) + i(ad + bc)) = \begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix}$

Kärnan $= \{a + ib: \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\} = \{0\}$

RA 28 a) $(r,0) - (s,0) = (r - s,0) \in RX\{0\}$ så $RX\{0\}$ är additiv delgrupp (se anm. efter lösningen till RA 3).

$(r,m)(s,0) = (s,0)(r,m) = (rs,0) \in RX\{0\}$, så $RX\{0\}$ är sluten under multiplikation med element i RXZ.

b) $f(x + y) = (x + y,0)$, $f(x) + f(y) = (x,0) + (y,0) = (x + y,0)$

$f(xy) = (xy,0)$, $f(x)f(y) = (x,0)(y,0) = (xy,0)$

c) Kärnan är $\{x: f(x) = (x,0) = (0,0)\} = \{0\}$ så f är en isomorfism.

d) $g((r,m)) = m$ är en isomorfism av $RXZ/RX\{0\}$ på Z för den är

i) Väldefinierad: $g((s,m)) = m$

ii) Homomorfism: $g((r,m) + (s,n)) = g((r + s,m + n)) = m + n =$

$= g((r,m)) + g((s,n))$ och $g((r,m)(s,n)) = g((rs + rn + sm,mn)) =$

$= mn = g((r,m))g((s,n))$

iii) Kärnan $= RX\{0\}$: Ker $g = \{(r,m): g((r,m)) = 0\} = \{(r,0)\} = RX\{0\}$

RA 29 a) $156 = 1 \cdot 91 + 65$

$91 = 1 \cdot 65 + 26$

$65 = 2 \cdot 26 + 13$

$26 = 2 \cdot 13$ så $13 = (156,91)$.

b) $13 = 65 - 2 \cdot 26$, men $26 = 91 - 65$ ger

$13 = 65 - 2(91 - 65) = 3 \cdot 65 - 2 \cdot 91$, men $65 = 156 - 91$ ger

$13 = 3(156 - 91) - 2 \cdot 91 = 3 \cdot 156 - 5 \cdot 91$

RA 31 a) $18m + 12n$ kan skrivas $3m + 2n = 1$. Eftersom $(3,2) = 1$ är en sådan framställning möjlig enligt RA 30 a.

b) $18m + 12n = 24$ kan skrivas $3m + 2n = 4$. Enligt ovan finns m_1 och n_1 så att $3m_1 + 2n_1 = 1$. Då gäller $3 \cdot 4m_1 + 2 \cdot 4n_1 = 4$.

c) $6 \mid (18m + 12n)$ men $6 \nmid 25$. Det finns alltså inte sådana heltal m och n.

RA 34 $(4,6) = 2$. Alltså finns m_1 och n_1 så $2 = 4m_1 + 6n_1$. Varje multipel av 2 är också en linjärkombination av 4 och 6 (multiplicera $2 = 4m_1 + 6n_1$). Å andra sidan är varje linjärkombination av 4 och 6 delbar med 2.

RA 36 $\{6a + 12b\} = 6\mathbb{Z}$ eftersom $(6,12) = 6$ så $\{6a + 12b + 15c\} = \{6d + 15c\} = 3\mathbb{Z}$

RA 38 $a \in b\mathbb{Z}$ så $a = bz$ för något $z \in \mathbb{Z}$, d.v.s. $b \mid a$. Men om $b \mid a$ så är varje multipel av b också en multipel av a. $a\mathbb{Z} \subseteq b\mathbb{Z}$ är alltså ekvivalent med att $b \mid a$.

RA 41 a) Om $A = R$ gäller $1 \in A$. Om $1 \in A$ gäller $1 \cdot r = r \in A$ för varje $r \in R$ d.v.s. $A = R$.

b) Om $A = R$ gäller $1 \in A$ (1 är invertibelt). Om $u \in A$ och u har inversen u^{-1} gäller $uu^{-1} = 1 \in A$ så $A = R$ enligt ovan.

RA 42 Om $nr = ns = 0$ gäller $n(r - s) = nr - ns = 0$, d.v.s. om $r,s \in R_n$ så gäller $r - s \in R_n$ så R_n är en additiv delgrupp (jfr anm. efter lösningen till RA 3). Om $nr = 0$ gäller $nsr = s(nr) = 0$ och $nrs = (nr)s = 0$ för varje $s \in R$ så R_n är sluten under multiplikation med element i R.

RA 47 a) Om $x^n \in A$ och $y^m \in A$ gäller $(x - y)^{n+m} \in A$ för $(x - y)^{n+m} = \Sigma \binom{n+m}{k} x^k (-y)^{n+m-k}$ och då är $k \geq n$ eller $n + m - k \geq m$ och varje term i summan och därmed hela summan tillhör A. Det finns alltså en potens av $x - y$ som tillhör A. Om $x^n \notin A$ gäller att $(rx)^n = r^n x^n \in A$ för varje $r \in R$. (Jfr anm. efter lösningen till RA 3.)

forts. RA

RA 47 b) Om $x \in A$ så gäller $x^n \in A$ för varje $n \geq 1$ t.o.m.

c) $N(A) \subseteq N(N(A))$ enligt ovan. Om $x \in N(N(A))$ gäller $x^n \in N(A)$ för något n. Men då gäller $(x^n)^m = x^{nm} \in A$. Det finns alltså en potens av x som tillhör A, d.v.s. $x \in N(A)$.

d) $N(A) = \{x \in Z: x^n$ är en multipel av 4 för något $n\} = 2Z$.

f) $N(A) = \{x \in Z: x^n$ är en multipel av $m = p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k}$, p_i olika primtal$\}$. d måste alltså innehålla varje primfaktor i m, och $d = p_1 p_2 \ldots p_k$ duger.

e) $12 = 2^2 \cdot 3$ ger $d = 2 \cdot 3 = 6$.

RA 52 a) $a \in P$ resp. $ab \in P$ är ekvivalent med $\bar{a} = 0$ resp. $\overline{ab} = 0$ i R/P.

b) Idealen i Z är av formen dZ. Primfaktoruppdela d. Om d ej är primtal är dZ ej primideal (man kan då hitta a,b med ab = d där varken a eller b delar p). Om däremot d är primtal är dZ primideal, för om ab har en faktor d, så har a eller b en faktor d.

c) M är maximalideal om och endast om R/M är en kropp. Men en kropp är speciellt ett integritetsområde, så M är ett primideal enligt a).

d) I ringen 2Z är 4Z ett maximalideal, för om ett ideal omfattar 4Z och dessutom ett tal 4m + 2, så omfattar det också 4m + 2 - 4m = 2 och därmed hela 2Z. Däremot är 4Z inte ett primideal för $2 \cdot 2 \in 4Z$ men $2 \notin 4Z$.

e) Låt P$\supset$ker f. Då är R/P isomorf med S/f(P) så R/P är ett integritetsområde (en kropp) om och endast om S/f(P) är ett integritetsområde (en kropp), d.v.s. P är ett primideal (maximalideal) om och endast om f(P) är ett primideal (maximalideal).

f) Om $x^n \in P$ gäller $x \cdot x^{n-1} \in P$ d.v.s. $x \in P$ eller $x^{n-1} \in P$ och med induktion $x \in P$.

RA 54 Idealet $(3, 2X^2 + 1)$ i $Z[X]$ svara mot idealet $\bar{2}X^2 + \bar{1}$ vid den naturliga homomorfismen av $Z[X]$ på $Z_3[X]$ (alla koefficienter reduceras modulo 3). Då är $Z[X]/(3, 2X^2 + 1)$ isomorf med $Z_3[X]/(\bar{2}X^2 + \bar{1})$. (Om $A \subsetneq B$ är två ideal i R gäller att R/B är isomorf med (R/A)/(B/A.)

RA 57 a) $X^3 + 3X^2 + 3X + 2 = (X^3 + 2X^2 + X + 2) + (X^2 + 2X)$

$X^3 + 2X^2 + X + 2 = X(X^2 + 2X) + X + 2$

$X^2 + 2X = X(X + 2)$ så $(X^3 + 2X^2 + X + 2, X^3 + 3X^2 + 3X + 2) = X + 2$

$X + 2 = (X^3 + 2X^2 + X + 2) - X(X^2 + 2X)$ men $X^2 + 2X = (X^3 + 3X^2 +$

$+ 3X + 2) - (X^3 + 2X^2 + X + 2)$ så

$X + 2 = (X^3 + 2X^2 + X + 2 - X((X^3 + 3X^2 + 3X + 2) - (X^3 + 2X^2 + X + 2)) =$

$= (1 + X)(X^3 + 2X^2 + X + 2) - X(X^3 + 3X^2 + 3X + 2)$

RA 61 a) Polynomet har ett nollställe $\bar{1}$ och alltså en faktor $X - \bar{1} = X + \bar{1}$. $X^4 + X^3 + X^2 + \bar{1} = (X + \bar{1})(X^3 + X + \bar{1})$. $X^3 + X + \bar{1}$ är irreducibelt eftersom det inte har något nollställe.

b) Polynomet har inget nollställe och alltså ingen förstagradsfaktor. Det enda irreducibla andragradspolynomet är $X^2 + X + \bar{1}$. Prövning ger $X^4 + X^2 + \bar{1} = (X^2 + X + \bar{1})^2$.

RA 63 a) Varje element i $Q[X]/(X^2 - 3)$ kan entydigt representeras som $\overline{a + bX}$. Avbilda detta element på $a + b\sqrt{3}$. Detta blir givetvis en additiv gruppisomorfism. $\overline{(a + bX)(c + dX)} = \overline{ac + (ad + bc)X + bdX^2} =$

$= \overline{ac + 3bd + (ad + bc)X + bd(X^2 - 3)} = \overline{ac + 3bd + (ad + bc)X}$ avbildas på $ac + 3bd + (ad + bc)\sqrt{3}$ vilket är lika med $(a + b\sqrt{3})(c + d\sqrt{3})$. Vi har visat att bilden av en produkt är produkten av bilderna. Avbildningens kärna är noll, så vi har en isomorfism.

Lösningar

RB 5 Låt $a \in G$. Betrakta $\{ab: b \in G\}$. Elementen i denna mängd är alla olika, för om $ab = ac$ gäller $a(b - c) = 0$ d.v.s. $b = c$ eftersom a är icke-nolldelare. Så $\{ab: b \in G\} = G$ eftersom alla ab är icke-nolldelare ($(ab)c = 0$ ger $a(bc) = 0$ ger $bc = 0$ eftersom a är icke-nolldelare, ger $c = 0$ eftersom b är icke-nolldelare). Eftersom $1 \in G$ finns b_1 så att $ab_1 = 1$. Associativiteten för multiplikation gäller allmänt i en ring.

RB 8 Låt C vara ett ideal, sådant att A/C är kommutativ. Då är $\overline{\overline{xy}} - \overline{\overline{yx}} = \overline{\overline{xy} - \overline{yx}} = 0$ för varje $x,y \in A$, d.v.s. $xy - yx \in C$ för varje $x,y \in A$. Å andra sidan, om varje $xy - yx \in C$, gäller $\overline{\overline{xy}} - \overline{\overline{yx}} = 0$, d.v.s. A/C kommutativ.

RB 9 En homomorf bild av Z_{pq} är en homomorf bild av Z, med en kärna som omfattar pqZ. De ideal som omfattar pqZ är: pqZ, pZ, qZ och Z. Möjliga bilder är alltså (bortsett från isomorfismer): Z_{pq}, Z_p, Z_q och nollringen.

RB 11 a) Det räcker att visa att R är sluten under subtraktion (se anm. efter lösningen till RA 3) och multiplikation. $a/b - c/d = (ad - bc)/bd$ och $(a/b)(c/d) = ac/bd$. Om $(b,p) = 1$ och $(d,p) = 1$ gäller $(bd,p) = 1$.

b) Låt $x = c/d \in Q$ vara förkortat. Antingen gäller $(d,p) = 1$, d.v.s. $x \in R$, eller $(c,p) = 1$, d.v.s. $x^{-1} \in R$.

c) Bryt ut maximal potens av p ur både täljare och nämnare i $a/b = p^n(a_1/b_1)$. Eftersom både $(a_1,p) = 1$ och $(b_1,p) = 1$ hör både a_1/b_1 och b_1/a_1 till R och $(a_1/b_1)(b_1/a_1) = 1$.

d) Låt S vara en delring till Q som är strikt större än R, och låt $c/d \in S \setminus R$. Förkorta så att $(c,p) = 1$. Låt $d = pd_1$. Då gäller $d_1/c \in R \subsetneq S$ och alltså $(d_1/c)(c/d) = 1/p \in S$ och därmed $1/p^n \in S$ för varje n. Varje element i $Q \setminus R$ kan skrivas $(1/p^n)r$ med $r \in R$, och därmed följer $S = Q$.

forts.

RB 11 e) a/b har inversen b/a om (a,p) = 1. Om $a = p^n a_1$, $n > 0$ och (b,p) = 1 har a/b ingen invers i R.

f) Låt A vara ett ideal. Låt m = min{n: a/b$\in$ A, a/b förkortat, $a = p^n a_1$ med $(a_1,p) = 1$}. Då är a_1/b invertibelt enligt e), så $(b/a_1)(a/b) = p^n \in A$. Då gäller $p^m R \subseteq A$, men inget element utanför $p^m R$ kan tillhöra A eftersom m = min{n}, så $A = p^m R$. De enda idealen i R är alltså $p^m R$, m = 0,1,2...

RB 12 b) Låt $f(ae + bj + ck + dl) = \begin{pmatrix} a+ib & c+id \\ -c+id & a-ib \end{pmatrix}$. Att detta är en additiv grupphomomorfism är klart. Ker f = {ae + bj + ck + dl: $\begin{pmatrix} a+ib & c+i \\ -c+id & a-i \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$} vilket ger $\begin{cases} a + b = 0 \\ a - b = 0 \end{cases}$ och $\begin{cases} c + d = 0 \\ -c + d = 0 \end{cases}$ vilket ger a = b = c = d = 0. Alltså en isomorfism.

$f((ae + bj + ck + dl)(a_1e + b_1j + c_1k + d_1l)) =$

$= f(aa_1 - bb_1 - cc_1 - dd_1 + (ab_1 + a_1b + cd_1 - c_1d)j +$

$+ (ac_1 + a_1c + b_1d - bd_1)k + (ad_1 + a_1d + bc_1 - b_1c)l) =$

$$\begin{pmatrix} aa_1-bb_1-cc_1-dd_1+i(ab_1+a_1b+cd_1c_1d) & ac_1+a_1c+b_1d-bd_1+i(ad_1+a_1d+bc_1-b_1c) \\ -(ac_1+a_1c+b_1d-bd_1)+i(ad_1+a_1d+bc_1-b_1c) & aa_1-bb_1-cc_1-dd_1-i(ab_1+a_1b+cd_1-c_1d) \end{pmatrix} =$$

$= \begin{pmatrix} a+ib & c+id \\ -c+id & a-ib \end{pmatrix} \begin{pmatrix} a_1+ib_1 & c_1+id_1 \\ -c_1+id_1 & a_1-ib_1 \end{pmatrix} =$

$= f(ae + bj + ck + dl)f(a_1e + b_1j + c_1k + d_1l).$

Alltså en ringisomorfism.

RB 14 a) 1) är kroppen Z_5. Att 2) är en kommutativ ring inses genast (den är en additiv grupp, och den är sluten under multiplikation). I 2) gäller: $\bar{6}\cdot\bar{0} = \bar{0}$, $\bar{6}\cdot\bar{2} = \bar{2}$, $\bar{6}\cdot\bar{4} = \bar{4}$, $\bar{6}\cdot\bar{6} = \bar{6}$, $\bar{6}\cdot\bar{8} = \bar{8}$. $\bar{6}$ är alltså enhetselement för multiplikation. Vidare gäller: $\bar{2}\cdot\bar{8} = \bar{6}$, $\bar{4}\cdot\bar{4} = \bar{6}$, $\bar{6}\cdot\bar{6} = \bar{6}$, så varje element $\neq \bar{0}$ har en invers. Även 2) är alltså en kropp. Betrakta avbildningen f från 1) till 2) definierad genom $f(\bar{0}) = \bar{0}$, $f(\bar{1}) = \bar{6}$, $f(\bar{2}) = \bar{2}$, $f(\bar{3}) = \bar{8}$, $f(\bar{4}) = \bar{4}$. Här gäller:

$f(\bar{0} + \bar{0}) = \bar{0} = \bar{0} + \bar{0} = f(\bar{0}) + f(\bar{0})$, $f(\bar{1} + \bar{0}) = \bar{6} = \bar{6} + \bar{0} = f(\bar{1}) + f(\bar{0})$,

$f(\bar{2} + \bar{0}) = \bar{2} = \bar{2} + \bar{0} = f(\bar{2}) + f(\bar{0})$, $f(\bar{3} + \bar{0}) = \bar{8} = \bar{8} + \bar{0} = f(\bar{3}) + f(\bar{0})$,

$f(\bar{4} + \bar{0}) = \bar{4} = \bar{4} + \bar{0} = f(\bar{4}) + f(\bar{0})$, $f(\bar{1} + \bar{1}) = \bar{2} = \bar{6} + \bar{6} = f(\bar{1}) + f(\bar{1})$,

forts.

RB 14 a) $f(\bar{2}+\bar{1}) = \bar{8} = \bar{2}+\bar{6} = f(\bar{2}) + f(\bar{1})$, $f(\bar{3}+\bar{1}) = \bar{4} = \bar{8}+\bar{6} = f(\bar{3}) + f(\bar{1})$, $f(\bar{4}+\bar{1}) = \bar{0} = \bar{4}+\bar{6} = f(\bar{4}) + f(\bar{1})$, $f(\bar{2}+\bar{2}) = \bar{4} = \bar{2}+\bar{2} = f(\bar{2}) + f(\bar{2})$, $f(\bar{3}+\bar{2}) = \bar{0} = \bar{8}+\bar{2} = f(\bar{3}) + f(\bar{2})$, $f(\bar{4}+\bar{2}) = \bar{6} = \bar{4}+\bar{2} = f(\bar{4}) + f(\bar{2})$ $f(\bar{3}+\bar{3}) = \bar{6} = \bar{8}+\bar{8} = f(\bar{3}) + f(\bar{3})$, $f(\bar{4}+\bar{3}) = \bar{2} = \bar{4}+\bar{8} = f(\bar{4}) + f(\bar{3})$ $f(\bar{4}+\bar{4}) = \bar{8} = \bar{4}+\bar{4} = f(\bar{4}) + f(\bar{4})$, $f(a\cdot\bar{0}) = f(\bar{0}) = \bar{0} = f(a)f(\bar{0})$ och $f(a\cdot\bar{1}) = f(a) = f(a)f(\bar{1})$ för varje a eftersom $f(\bar{0}) = \bar{0}$ och $f(\bar{1}) = \bar{6}$ = enhetselementet i 2). Vidare är: $f(\bar{2}\cdot\bar{2}) = \bar{4} = \bar{2}\cdot\bar{2} = f(\bar{2})f(\bar{2})$, $f(\bar{2}\cdot\bar{3}) = \bar{6} = \bar{2}\cdot\bar{8} = f(\bar{2})f(\bar{3})$, $f(\bar{2}\cdot\bar{4}) = \bar{8} = \bar{2}\cdot\bar{4} = f(\bar{2})f(\bar{4})$, $f(\bar{3}\cdot\bar{3}) = \bar{4} = \bar{8}\cdot\bar{8} = f(\bar{3})f(\bar{3})$, $f(\bar{3}\cdot\bar{4}) = \bar{2} = \bar{8}\cdot\bar{4} = f(\bar{3})f(\bar{4})$ samt $f(\bar{4}\cdot\bar{4}) = \bar{6} = \bar{4}\cdot\bar{4} = f(\bar{4})f(\bar{4})$ vilket visar att f är en isomorfism.

RB 16 a) $h(mn) = \underbrace{e+e+\ldots+e}_{mn \text{ termer}} = (\underbrace{e+e+\ldots+e}_{m \text{ termer}})(\underbrace{e+e+\ldots+e}_{n \text{ termer}}) = h(m)h(n)$ för varje m och n.

b) Varje homomorf bild av Z är isomorf med Z eller Z_n för något n, eftersom varje homomorf bild av Z är isomorf med Z/kärnan, och kärnan är ett ideal i Z.

RB 18 Låt n vara ordningen av ringens etta $\bar{1}$. Då gäller $na = (\underbrace{\bar{1}+\bar{1}+\ldots+\bar{1}}_{n \text{ termer}})a = 0$ för varje a. Ettan i ringen har alltså maximal ordning och är därmed generator för den additiva gruppen. Definiera nu en avbildning från R till Z_n genom $f(k\cdot\bar{1}) = k$ där k är ett heltal sådant att $0 \leq k \leq n-1$. Denna avbildning är en isomorfism för den är: i) väldefinierad (varje element i R har en entydig framställning som $k\cdot\bar{1}$ med $0 \leq k < n$ eftersom 1 genererar den additiva gruppen), ii) självklart homomorfism samt iii) har kärnan $\{0\cdot\bar{1}\}$.

RB 19 Att M är en additiv delgrupp är klart. $\begin{pmatrix} a & c \\ 0 & a \end{pmatrix}\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & ab \\ 0 & 0 \end{pmatrix}$ och $\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & c \\ 0 & a \end{pmatrix} = \begin{pmatrix} 0 & ab \\ 0 & 0 \end{pmatrix}$ visar att M är ett ideal. R/M blir isomorf med $\{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}: a \in Q\}$ som är isomorf med Q, d.v.s. R/M är en kropp och M således ett maximalideal.

RB 20 Eftersom $p^nR \supseteq p^{n+1}R$ är pR det enda maximalidealet.

RB 22 a) Ett primelement i 2Z kan inte vara delbart med 4. Å andra sidan kan man inte uppdela ett element $4k + 2$ i 2Z.

b) En Euklidisk ring har speciellt en etta, vilket 2Z inte har.

c) Låt A vara ett ideal $\neq 0$. Om a är det minsta positiva heltalet i A (sådana finns, för om $b \in A$ så gäller $-b \in A$) så måste $a \cdot 2Z \subseteq A$. Men om A vore strikt större än $a \cdot 2Z$, så funnes ett $b \in A \setminus a \cdot 2Z$. Man kan anta att $b > 0$. Låt $a \cdot 2n$ vara den största positiva jämna multipel av a som är mindre än b. Då gäller $b - a \cdot 2n \in A$, men $0 < b - a \cdot 2n < a$. Motsägelse.

RB 23 a) Låt $N(a + ib) = a^2 + b^2$. Då gäller $N(z_1z_2) = N(z_1)N(z_2)$. Ett element z är invertibelt om och endast om $N(z) = 1$. $N(7i - 4) = 16 + 49 = 65 = 5 \cdot 13$. Möjlig uppdelning av $7i - 4$ är ab där $N(a) = 5$, $N(b) = 13$. Prövning ger $7i - 4 = (1 + 2i)(3i + 2)$. Denna uppdelning är unik, bortsett från ordning och invertibla element $(1, -1, i, -i)$.

b) $N(9 + 4i) = 81 + 16 = 97$ som är primtal i Z. Alltså är $9 + 4i$ primtal i $Z[i]$.

RB 24 a) $9 - 2i = 1(6 + 2i) + (3 - 4i)$

$6 + 2i = i(3 - 4i) + (2 - i)$

$3 - 4i = (2 - i)(2 - i)$ så $(9 - 2i, 6 + 2i) = 2 - i$

$2 - i = (6 + 2i) - i(3 - 4i)$ men $3 - 4i = (9 - 2i) - (6 + 2i)$ så

$2 - i = (6 + 2i) - i((9 - 2i) - (6 + 2i)) = (1 + i)(6 + 2i) - i(9 - 2i)$

RB 25 a) Det ideal som genereras av $6 + 2i$ och $9 - 2i$ är det ideal som genereras av största gemensamma delaren, d.v.s. $(2 - i)\,\mathbb{Z}[i]$.

RB 26 a) De tal, som är multipler av både $6 + 2i$ och $9 - 2i$ är de tal som är multipler av $(6 + 2i)(9 - 2i)/(6 + 2i, 9 - 2i) = 22 + 14\,i$.

RB 27 a) $2 + i$ är primelement ($N(2 + i) = 5$, primtal) så $(2 + i)\mathbb{Z}$ i är ett maximalideal.

b) Det minsta positiva rationella heltal som är en multipel av $2 + i$ är 5, så den minsta rationella heltalsmultipeln av 1 som är noll, är 5.

c) Elementen kan representeras av element med norm < 5 (detta inses med Euklides algoritm). Elementen blir: $\overline{2} = \overline{2} - \overline{(2 + i)} = \overline{2} + \overline{(i - 1)}\,\overline{(2 + i)}$, $\overline{1} = \overline{1} - \overline{(2 + i)} = \overline{1} + \overline{i}\,\overline{(2 + i)}$, $\overline{0}$, $\overline{1 + i} = \overline{1 + i} - \overline{(2 + i)} =$ $= \overline{1 + i} + \overline{(-i - 1)}\,\overline{(2 + i)}$, $\overline{1 - i} = \overline{1 - i} + \overline{i}\,\overline{(2 + i)} = \overline{1 - i} + \overline{(i - 1)}\,\overline{(2+i)}$. Ovan är restklasserna till samtliga 13 element med norm < 5 uppräknade. De gav upphov till 5 olika element i restklassringen. (Denna är alltså isomorf med $\mathbb{Z}_5$.)

RB 30 Eftersom $\mathbb{Z}[i]$ är en Euklidisk ring, är idealen principala. $a\mathbb{Z}[i] \subseteq b\mathbb{Z}[i]$ om och endast om b delar a. Ett ideal är maximalt precis då det genereras av ett primtal i $\mathbb{Z}[i]$. Den enda primfaktorn i 2 är $1 + i$ (och dess associerade).

RB 31 a) $N((a + b\sqrt{-2})(c + d\sqrt{-2})) = N(ac - 2bd + (ad + bc)\sqrt{-2}) = (ac - 2bd)^2 + 2(ad + bc)^2 = a^2c^2 - 4abcd + 4b^2d^2 + 2a^2d^2 + 4abcd + 2b^2c^2$.
$N(a + b\sqrt{-2})N(c + d\sqrt{-2}) = (a^2 + 2b^2)(c^2 + 2d^2) = a^2c^2 + 2a^2d^2 +$
$+ 2b^2c^2 + 4b^2d^2$.

b) Om $xy = 1$ är $N(xy) = N(x)N(y) = N(1) = 1$. Eftersom $N(x)$ är ett heltal ≥ 0 måste $N(x) = 1$. Om å andra sidan $N(a + b\sqrt{-2}) = a^2 + 2b^2 =$ $= (a + b\sqrt{-2})(a - b\sqrt{-2}) = 1$ är $a + b\sqrt{-2}$ invertibelt med invers $a - b\sqrt{-2}$. De invertibla elementen är alltså de som har norm = 1, d.v.s. 1 och -1.

forts.

RB 31 c) Om ett element har primtalsnorm är elementet primt. T.ex. är $1 + \sqrt{-2}$ med norm 3 primt.

d) Om x och y är två element $\neq 0$ i $Z[\sqrt{-2}]$ gäller det att finna $q \in Z[\sqrt{-2}]$ så $N(x - qy) < N(y)$. Om man utvidgar $Z[\sqrt{-2}]$ till sin kvotkropp gäller fortfarande $N(xy) = N(x)N(y)$. I kvotkroppen finns ett element $q_1 = a_1 + b_1\sqrt{-2}$ så att $x - q_1y = 0$ (tag $q_1 = x/y$). Välj $q = a + b\sqrt{-2}$, där a resp. b ligger så nära a_1 resp. b_1 som möjligt. Då gäller $N(x - qy) = N(x - q_1y + (q_1 - q)y) = N((q_1 - q)y) = N(q_1 - q)N(y) \leq ((1/2)^2 + 2(1/2)^2)N(y) < N(y)$.

RB 36 a) Polynomet har nollställena $\bar{1}$ och $\bar{2}$ vilket ger uppdelningen $(X + \bar{1})(X + \bar{2})(X^2 + \bar{2}X + \bar{2})$. $X^2 + \bar{2}X + \bar{2}$ saknar nollställen och är alltså irreducibelt.

b) Polynomet saknar nollställen. Prövning med de irreducibla andragradspolynomen ger uppdelningen $(X^2 + \bar{1})(X^2 + \bar{2}X + \bar{2})$.

RB 38 a) $X^3 + \bar{4}X + \bar{2} = (X^3 - +X^2 + \bar{2}X + \bar{5}) + (\bar{2}X^2 + \bar{2}X - \bar{3})$

$X^3 - \bar{2}X^2 + \bar{2}X + \bar{5} = (\bar{6}X + \bar{4})(\bar{2}X^2 + 2X - \bar{3}) + (X + \bar{6})$

$\bar{2}X^2 + \bar{2}X - \bar{3} = (\bar{2}X + \bar{1})(X + \bar{6}) + \bar{2}$ vilket ger

$\bar{2} = (\bar{2}X^2 + \bar{2}X - \bar{3}) - (\bar{2}X + \bar{1})(X + \bar{6})$ men $X + \bar{6} = (X^3 - \bar{2}X^2 + \bar{2}X + \bar{5}) -$

$- (\bar{6}X + \bar{4})(\bar{2}X^2 + \bar{2}X - \bar{3})$ så

$\bar{2} = (\bar{2}X^2 + \bar{2}X - \bar{3}) - (\bar{2}X + \bar{1})((X^3 - \bar{2}X^2 + \bar{2}X + \bar{5}) - (\bar{6}X + \bar{4})(\bar{2}X^2 + +X - \bar{3}))$

$= (X^2 + \bar{3}X + \bar{5})(\bar{2}X^2 + \bar{2}X - \bar{3}) - (\bar{2}X + \bar{1})(X^3 - \bar{2}X^2 + \bar{2}X + \bar{5})$ men

$\bar{2}X^2 + \bar{2}X - \bar{3} = (X^3 + \bar{4}X + \bar{2}) - (X^3 - \bar{2}X^2 + \bar{2}X + \bar{5})$ så

$\bar{2} = (X^2 + \bar{3}X + \bar{5})((X^3 + \bar{4}X + \bar{2}) - (X^3 - \bar{2}X^2 + \bar{2}X + \bar{5})) -$

$- (\bar{2}X + \bar{1})(X^3 - \bar{2}X^2 + \bar{2}X^2 + \bar{2}X + \bar{5}) =$

$= (X^2 + \bar{3}X + \bar{5})(X^3 + \bar{4}X + \bar{2}) - (X^2 + \bar{5}X + \bar{6})(X^3 - \bar{2}X + \bar{2}X + \bar{5})$ eller

eftersom $\bar{2} \cdot \bar{6} = \bar{1}$

$\bar{1} = (\bar{6}X^2 + \bar{7}X + \bar{8})(X^3 + \bar{4}X + \bar{2}) - (\bar{6}X^2 + \bar{8}X + \bar{3})(X^3 - \bar{2}X^2 + \bar{2}X + \bar{5})$

RB 40 a) $X^2 + 5$ är irreducibelt så $(X^2 + 5)\mathbb{Q}[X]$ är ett maximalideal, så $\mathbb{Q}[X]/(X^2 + 5)$ är en kropp.

b) Elementen har representanter som är polynom av grad högst 1, och alla sådana polynom representerar olika kroppselement. Antalet sådana polynom är $13^2 = 169$.

c) Z_{13} har karaktäristik 13 och därmed också $Z_{13}[X]/(X^2 + \bar{5})$

d) Euklides algoritm i $Z_{13}[X]$ ger
$\bar{1} = (\bar{8}X^3 + \overline{10}X + \bar{8})(X^2 + \bar{5}) + \bar{5}X(X^4 + \bar{3}X^2 + X + \bar{3})$, vilket modulo $(X^2 + \bar{5})$ ger att $\bar{5}X$ representerar inversen till $X^4 + \bar{3}X^2 + X + \bar{3}$.

RB 42 a) $X^2 + \bar{3}X + \bar{2} = (X + \bar{1})(X + \bar{2})$. Elementen i $Z_5[X]/(X^2 + \bar{3}X + \bar{2})$ svarar en-entydigt mot polynomen av grad ≤ 1 i $Z_5[X]$. Ett sådant polynom representerar en nolldelare precis då den har en primtalsfaktor gemensam med $X^2 + \bar{3}X + \bar{2}$. (Om $p(X) = f(X)g(X)$, och $X^2 + \bar{3}X + \bar{2} = f(x)h(X)$ gäller $p(X)h(X) = \bar{0}$. Om $p(X)$ inte har någon primtalsfaktor gemensam med $X^2 + \bar{3}X + \bar{2}$, så har $p(X)$ t.o.m. en invers, vilket inses med Euklides algoritm.) Antalet sådana är 8, nämligen:
$a(X + \bar{1})$ samt $a(X + \bar{2})$ där $a = \bar{1}, \bar{2}, \bar{3}$ eller $\bar{4}$.

RB 43 a) Idealen i $R = Z_5[X]/(X^2 + \bar{3}X + \bar{2})$ svarar en-entydigt mot idealen i $Z_5[X]$ som omfattar $(X^2 + 3X + 2)Z_5[X]$. I $Z_5[X]$ är varje ideal principalt och $aZ_5[X] \supseteq bZ_5[X]$ precis då a delar b. Antalet delare till $X^2 + \bar{3}X + \bar{2}$ (bortsett från associerade som ju ger upphov till samma ideal) är 4, nämligen $\bar{1}$, $X + \bar{1}$, $X + \bar{2}$ och $(X + \bar{1})(X + \bar{2})$. I R svarar dessa mot resp. R, $(X + \bar{1})R$, $(X + \bar{2})R$, och nollidealet.

RB 44 a) Varje element i $Z_3[X]$ kan skrivas som $f(X) = g(X)(X + \bar{1}) + c$. Definiera en avbildning från $Z_3[X]$ till Z_3 genom $F(f(X)) = c$. Denna avbildning är en homomorfi, eftersom summan av rester är resten av summan, och produkten av resterna är resten av produkten. Kärnan är $(X + \bar{1})Z_3[X]$. $Z_3[X]/(X + \bar{1})$ är alltså isomorf med Z_3. På samma sätt visas att $Z_3[X]/(X - \bar{1})$ är isomorf med Z_3.

forts.

RB 44 b) $Z_3[X]/(X^2 + \bar{1})$ är en kropp, eftersom $(X^2 + \bar{1})$ är irreducibelt. $Z_3[X]/(X^2 - \bar{1})$ har t.o.m. nolldelare (t.ex. bilden av $X + \bar{1}$). De kan alltså inte vara isomorfa.

RB 45 Med Euklides algoritm visas att största gemensamma delare till de två polynomen är 1. Det ideal, som genereras av två polynom, är det ideal som genereras av största gemensamma delare till polynomen. I detta fall fås alltså hela $Q[X]$.

RB 46 Med Euklides algoritm fås $(2X^4 + 2X^3 + 3X^2 + X + 1,\ 6X^3 - 4X^2 + 3X - 2) = 2X^2 + 1$. Det ideal, som genereras av de två givna polynomen är alltså $(2X^2 + 1)Q[X]$. Detta ideal är maximalt eftersom $2X^2 + 1$ är irreducibelt.

RB 52 a), b) Idealen i $C[X]$ och $Q[X]$ är principala, och ett ideal omfattar ett annat precis då generatorn för det första idealet delar generatorn för det andra idealet. Ett ideal är maximalt precis då det genereras av ett irreducibelt element. Detta ger idealen $(X + i\sqrt{2})C[X]$ eller $(X - i\sqrt{2})C[X]$ i $C[X]$, och $(X^2 + 2)Q[X]$ i $Q[X]$.

c) Idealet $(2,X)$ omfattar $(X^2 + 2)$. $(2,X)$ är ett maximalideal, för $Z[X]/(2,X)$ är isomorf med Z_2 som är en kropp.

RB 53 $2X - 1 = 2(X - 2) + 3$, så $3 \in (2X - 1,\ X - 2)$ och $2X - 1 \in (X - 2,\ 3)$. Alltså är $(2X - 1,\ X - 2) = (3,\ X - 2)$. Antag att $1 \in A$ d.v.s. $1 = f(X)\cdot 3 + g(X)(X - 2)$. Insättning av $X = 2$ (d.v.s. homomorfin $f(X) \to f(2)$) ger motsägelse.

Lösningar

RC 1 Det måste gälla att 1 = 0 eller 2 = 0 eller 3 = 0, för om varken 1, 1 + 1 eller 1 + 1 + 1 = 0 gäller $2 \cdot 2 = 4 \neq 1$. Att nollringen, Z_2 och Z_3 uppfyller kraven inses genast. Om man nu bortser från nollringen, måste en ring som uppfyller kraven innehålla en delring isomorf med Z_2 eller Z_3. Antag det första fallet. Om ringen innehåller ytterligare ett element a ger $(a + 1)^2 = a^2 + 2a + 1 = 1 + 0 + 1 = 0$ en motsägelse ($a + 1 \neq 0$ skulle medföra $(a + 1)^2 = 1$). Antag det andra fallet. Om ringen innehåller ytterligare ett element a ger $(a + 1)^3 = a^3 + 3a + 1 =$ $= a \cdot 1 + 0 + 0 + 1 = a + 1$ en motsägelse.

RC 3 a) i) medför ii): Om u har en invers u^{-1} gäller $u_1 = 1 \cdot u_1 = (u^{-1}u)u_1 =$ $= u^{-1}(uu_1) = u^{-1} \cdot 1 = u^{-1}$ så $u^{-1} = u_1$ är den enda högerinversen.

ii) medför iii): Eftersom u inte har invers är $u_1 u \neq 1$. Men $u(1 - u_1 u) = u - (uu_1)u = u - 1 \cdot u = 0$.

iii) medför i): Om $uv = 0$, $v \neq 0$, är $u(u_1 + v) = uu_1 + uv = 1 + 0 = 1$ så $u_1 + v$ är också högerinvers.

b) $\{uu_1 r: r \in R\} = R$ för $uu_1 = 1$. Eftersom alla $uu_1 r$ är olika, är alla $u_1 r$ olika och $\{u_1 r\} = R$. Speciellt finns $s \in R$ så $u_1 s = 1$. Nu är $s = 1 \cdot s = (uu_1)s = u(u_1 s) = u \cdot 1 = u$, så u_1 är invers till u. Enligt a) är då u_1 den enda högerinversen.

RC 4 En grupp av primtalsordning har bara triviala delgrupper, så A har bara triviala ideal (ett ideal är ju speciellt en additiv delgrupp). Låt $a \in A$ vara sådant att $ab \neq 0$ för något $b \in A$. $\{ra: r \in A\}$ är ett ideal $\neq 0$ och alltså = A. Speciellt finns $s \in A$ så $sa = a$. Men s är etta i ringen, för varje element i ringen kan skrivas ar, och $s(ar) = (sa)r = ar$. Ettan genererar en additiv delgrupp som = A eftersom den är $\neq 0$. Som additiv

forts.

RC 4 grupp är alltså A isomorf med Z_p för något p. Men då är A som ring isomorf med Z_p ((1+1+...+1)(1+1+...+1) = 1+1+...+1).
m element n element mn element

RC 7 a) Att A är en additiv delgrupp till hela matrisringen följer av att A är sluten under subtraktion (se anm. efter lösningen till RA 3). Att A är sluten under multiplikation (som är kommutativ) följer av att $\begin{pmatrix} x & 0 \\ y & x \end{pmatrix} \begin{pmatrix} u & 0 \\ v & u \end{pmatrix} = \begin{pmatrix} u & 0 \\ v & u \end{pmatrix} \begin{pmatrix} x & 0 \\ y & x \end{pmatrix} = \begin{pmatrix} xu & 0 \\ yu+xv & xu \end{pmatrix}$.

b) Antag att ett ideal I innehåller en matris $\begin{pmatrix} x & 0 \\ y & x \end{pmatrix}$, och att $x \neq 0$. Multiplicera denna matris med $\begin{pmatrix} x & 0 \\ -y & x \end{pmatrix}$. Produkten blir en diagonalmatris med diagonal element $\neq 0$. Denna diagonal matris tillhör också I. Genom att multiplicera denna diagonalmatris med en annan lämplig diagonalmatris, inses att enhetsmatrisen (ringens etta) tillhör I. I är alltså hela ringen. Kvar att undersöka är mängden av matriser $\begin{pmatrix} 0 & 0 \\ y & 0 \end{pmatrix}$. Denna mängd bildar ett ideal, för den är sluten under subtraktion och multiplikation. Den kan heller inte innehålla några delmängder, som är ideal, för så fort en matris $\begin{pmatrix} 0 & 0 \\ y & 0 \end{pmatrix}$ med $y \neq 0$ ingår i ett ideal, så ingår alla (multiplicera med en lämplig diagonalmatris).

RC 10 a) Antag att ett ideal $I \neq 0$. Då finns en matris i I med åtminstone en koefficient $\neq 0$. Genom att multiplicera denna matris med en lämplig matris kan man få en matris med precis en kofficient $\neq 0$, och denna koefficient är en etta. Genom att multiplicera denna nya matris med lämpliga matriser, kan man få denna etta att flyttas till vilken annan plats som helst. Speciellt ingår alltså $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ och $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ i I. Därmed ingår också $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ i I, och I = hela ringen.

RC 14 a) $A \cap A = A$ för varje A.

forts.

RC 14 b) $(x + x)^2 = x^2 + x^2 + x^2 + x^2 = x + x + x + x$, men å andra sidan är $(x + x)^2 = x + x$ så $x + x = 0$ för varje x. $(x + y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y$. Men å andra sidan är $(x + y)^2 = x + y$ så $xy + yx = 0$ d.v.s. $xy = yx$ (eftersom $-yx = yx$) för varje x och y.

c) $xy(x + y) = xyx + xy^2 = x^2y + xy^2 = xy + yx = xy + xy = 0$ enligt a). Eftersom nolldelare saknas måste $xy = 0$ eller $x + y = 0$. Om x och y båda är skilda från 0 måste alltså $x = y$, och ringen är isomorf med Z_2.

RC 15 a) Mängden är sluten under multiplikation, för om $\lim x_n = 0$ och $\lim y_n = c$ gäller $\lim x_n y_n = 0$. Mängden är sluten under subtraktion, för om $\lim x_n = 0$ och $\lim y_n = 0$ gäller $\lim(x_n - y_n) = 0$ och I är ett ideal (se anm. efter lösningen till RA 3).

b) Definiera en avbildning F genom $F((x_n)) = \lim x_n$ från R till R. F är en homomorfi eftersom $\lim((x_n) + (y_n)) = \lim(x_n) + \lim(y_n)$ och $\lim(x_n y_n) = \lim(x_n)\lim(y_n)$. Kärnan är $\{(x_n)\colon \lim x_n = 0\}$ som är ett maximalideal eftersom R är en kropp.

RC 22 Vid en homomorf avbildning avbildas 1 på $\bar{1}$. Vidare gäller att $i^2 = -1$ avbildas på $-\bar{1} = \bar{4}$. i måste alltså avbildas på ett element med kvadrat $\bar{4}$. Möjliga bilder för i är då $\bar{2}$ och $\bar{3}$. Det räcker att känna bilderna av 1 och i för att hela avbildningen ska vara bestämd. Att avbildningarna f och g definierade genom $f(a + ib) = \overline{a + 2b}$ resp. $g(a + ib) = \overline{a + 3b}$ är additiva grupphomomorfismer inses genast. $f((a + ib)(c + id)) =$
$= f(ac - bd + i(ad + bc)) = \overline{ac - bd + 2(ad + bc)} = \overline{ac} + \overline{4bd} + 2(\overline{ad + bc}) =$
$= (\overline{a + 2b})(\overline{c + 2d}) = f(a + ib)f(c + id)$. $g((a + ib)(c + id)) =$
$= g(ac - bd + i(ad + bc)) = \overline{ac - bd + 3(ad + bc)} = \overline{ac} + \overline{9bd} + \overline{3(ad + bc)} =$
$= (\overline{a + 3b})(\overline{c + 3d}) = g(a + ib)g(c + id)$. Både f och g är ringhomomorfismer.

RC 25 Polynomet har nollstället $-\bar{1}$, och det ger en uppdelning
$X^4 + X^3 + \bar{3}X^2 + \bar{2} = (X + \bar{1})(X^3 - \bar{2}X + \bar{2})$. $X^3 - \bar{2}X + \bar{2}$ saknar nollställen

forts.

RC 25 och är alltså invertibelt. Elementen i R kan representeras av polynom av grad ≤ 3, och alla sådana polynom representerar olika element i R. Det finns alltså 5^4 element i R. Polynomet p(X) i $Z_5[X]$ representerar ett invertibelt element i R om och endast om det är relativt primt till $X^4 + X^3 + \bar{3}X^2 + \bar{2}$, för $\bar{1}$ är en linjärkombination av p(X) och $X^4 + X^3 + \bar{3}X^2 + \bar{2}$ precis då dessa polynom är relativt prima. Det finns 5 polynom av grad ≤ 3 som är delbara med $X^3 - \bar{2}X + \bar{2}$ och det finns 5^3 som är delbara med $X + \bar{1}$, och det är bara nollpolynomet som är delbart med båda. Det finns alltså $5^4 - 5^3 - 5 + 1 = 496$ invertibla element i R. Idealen i R svarar mot idealen i $Z_5[X]$ som omfattar $(X^4 + X^3 + \bar{3}X^2 + \bar{2})Z_5[X]$. De senare idealen är: $(X^4 + X^3 + \bar{3}X^2 + \bar{2})Z_5[X]$, $(X^3 - \bar{2}X + \bar{2})Z_5[X]$, $(X + 1)Z_5[X]$ och hela $Z_5[X]$.

RC 26 a) $XY - X = X(Y - 1)$ där X och $Y - 1$ är irreducibla eftersom de är av grad 1. $XY + Y + 1 = X(Y - 1) + (Y - 1) + X + 2$ är inte delbart med $Y - 1$ eftersom $X + 2$ inte är delbart med $Y - 1$. $XY + Y + 1$ är heller inte delbart med X. Alltså saknar de två polynomen gemensamma faktorer.

b) Antag att $(XY + Y + 1, XY - X) = Q[X,Y]$. Då finns polynom q(X,Y) och r(X,Y) i $Q[X,Y]$ sådana att $q(X,Y)(XY + Y + 1) + r(X,Y)(XY - X) = 1$. Ersätts Y med 1 (egentligen: gör avbildningen $f(X,Y) \to f(X,1)$, som är en homomorfi) fås $q(X,1)(2X + 1) = 1$ vilket uppenbarligen är omöjligt.

RC 27 $Z[X,Y]/(2,X^3 + X + 1)$ är isomorf med $Z_2[X,Y]/(X^3 + X + \bar{1})$ som är isomorf med $(Z_2[X]/(X^3 + X + \bar{1}))[Y]$ (reducera koefficienterna). $X^3 + X + \bar{1}$ saknar nollställen i $Z_2[X]$ och är alltså irreducibelt, vilket ger att $Z_2[X]/(X^3 + X + \bar{1})$ är en kropp. En polynomring över en kropp är en Euklidisk ring, och har speciellt entydig faktorisering.

Uppgifter

KA 1 Visa att $Z_n = Z/nZ$ är en kropp omm n är ett primtal.

KA 2 Låt $f:K \to A$ vara en ringhomomorfism $\neq 0$ av kroppen K in i ringen A. Visa att f är 1 - 1 (Ker f = 0).

KA 3 Låt K vara en kropp av karaktäristik $p > 0$. Visa att $a \to a^p$ definierar en isomorfism av K på en delkropp.
Ledning: Visa först att $(a + b)^p = a^p + b^p$.

KA 4 Bestäm $[\mathbb{C}:\mathbb{R}]$, $[\mathbb{R}:\mathbb{Q}]$, $[\mathbb{Q}(\sqrt[3]{2},i):\mathbb{Q}]$, $[\mathbb{Q}(\sqrt{3}/i):\mathbb{Q}]$.

KA 5 Visa att en ändlig kroppsutvidgning är algebraisk. Ge exempel på att omvändningen inte är sann.

KA 6 Visa att $K = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6};\ a,b,c,d \in \mathbb{Q}\}$ är en delkropp till C. Visa att K är algebraisk över Q och beräkna $[K:\mathbb{Q}]$.

KA 7 Vilken grad har en rot till ekvationen $x^4 + x^3 + x^2 + x + 1 = 0$ över kroppen $\mathbb{Q}(\sqrt{5})$?

KA 8 Vilken grad har $\sqrt[3]{2} - \sqrt{5}$ över Q?

KA 9 Visa att $\cos \pi/12$ är algebraiskt över Q.

KA 10 a) Skriv $(\sqrt[3]{2} + 1)^{-1}$ som polynom i $\sqrt[3]{2}$.
b) Skriv $\sqrt{2}$ som polynom i $\sqrt{2} + \sqrt{3}$.

KA 11 a) Bestäm $[\mathbb{Q}(\sqrt[3]{3} \cdot \sqrt[6]{4}):\mathbb{Q}]$, $[\mathbb{Q}((\sqrt{2} + \sqrt{3})^{-1}):\mathbb{Q}]$.
b) Bestäm $[\mathbb{Q}(\sqrt[4]{2},\sqrt{2}):\mathbb{Q}]$, $[\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}(\sqrt{2})]$, $[\mathbb{Q}(\sqrt[4]{2},i\sqrt{2}):\mathbb{Q}]$, $[\mathbb{Q}(\sqrt{2}, \cos \pi/4):\mathbb{Q}]$.
c) Bestäm $[\mathbb{Q}(X):\mathbb{Q}(X^2 + 1)]$ där $\mathbb{Q}(X)$ är kroppen av rationella funktioner i variabeln X över Q.

KA 12 a) Antag att $F(a) = F(b)$ och grad a = n (över F). Visa att grad b = n.

b) Antag att grad a = n. Visa att också grad a^{-1} = n.

KA 13 a) Hur definieras en ändlig kroppsutvidgning $F \subset K$ och vad menas med graden av K över F?

b) Bestäm graden av $Q(2^{2/3})$ över Q.

c) Bestäm graden av $Q((\sqrt{2} - 1)^{1/2})$ över Q.

KA 14 Bestäm minimalpolynomet över Q till $e^{2\pi i/n}$, n = 3, 4, 5 och 6. Vad händer om Q ersättes med R?

KA 15 Ange graden över Q av kropparna $Q(\sqrt[3]{6}, i\sqrt{6})$ och $Q(\sqrt[3]{6}, \sqrt{6}, i)$ (med kortfattade motiveringar).

KA 16 Visa att det finns ett 5-gradspolynom med rationella koefficienter som har $1 + \sqrt[5]{2} + 3 \cdot \sqrt[5]{8}$ som rot.

KA 17 Bestäm $[Z_p(i):Z_p]$ där i är en rot till $X^2 + 1 = 0$ och p = 3, 5, 11, 17.

KA 18 Låt α vara en rot till $X^3 + X^2 + 1$. Vilka värden kan $[Z_p(\alpha):Z_p]$ anta om p = 3, 5?

KA 19 a) Visa att $X^3 + 2X + 2$ är irreducibelt i $Z_3[X]$.

b) Visa att det finns en kropp med 27 element.

KA 20 a) Bevisa att för varje kropp F och varje polynom $f(X) \in F[X]$ existerar en utvidgning av F i vilken f(X) har minst en rot.

b) Beskriv rotkroppen för $X^3 - 2$ över Q. Vilken är dess grad över Q?

KA 21 Bestäm graden för en rotkropp (uppspaltningskropp) över Q till följande polynom $X^4 - 1$, $X^4 + 1$, $X^6 + 1$, $X^4 + 2$, $X^5 - 1$.

KA 22 Bestäm graden för en rotkropp till polynomet $X^6 - 3$ över Q.

KA 23 a) Bestäm graden för en rotkropp till polynomet $X^3 + X + 1$ över Z_3, Q, R.

b) Samma uppgift för $X^4 + X^3 + X^2 + X + 1$ över Q, R, Z_5.

KA 24 Låt $f \in R[X]$. Vilka olika grader över R för en rotkropp till f är möjliga?

Uppgifter

KB 1 Visa att en ändlig kropp måste ha p^n element där p är ett primtal.

KB 2 Visa att $\{0, 2, 4, 6, 8 \pmod{10}\}$ bildar en kropp. Enhetselement?

KB 3 Antag att $[F:K] = p$, p primt. Visa att $F = K(a)$ för godt. $a \in F - K$.

KB 4 a) Vilken grad har $Q(i,\sqrt{3})$ över Q?

b) Bestäm ett komplext tal γ så att $Q(i,\sqrt{3}) = Q(\gamma)$.

KB 5 Talet $\xi = \sqrt{2} + \sqrt[3]{3}$ är algebraiskt över Q. Sätt graden $[Q(\xi):Q] = n$.

a) Bevisa olikheterna $1 < n \leq 6$.

b) Bevisa att $n = 6$. (Resultatet i (a) får användas.)

KB 6 Antag att grad a över F är udda. Visa att $F(a) = F(a^2)$.

KB 7 Vilka möjligheter finns det för antalet element i kroppen $K(\xi)$ om K är kroppen med två element och ξ är en rot till ekvationen $x^5 + x + 1 = 0$.

KB 8 a) Visa att det finns en kropp K med 81 element. Ledning: Visa att t.ex. $x^4 + x^3 + x^2 + 1$ är ett irreducibelt polynom i $Z_3[x]$.

b) Visa att K inte har någon delkropp med 27 element.

c) Visa att $L = \{a \in K: a^9 = a\}$ är en delkropp med 9 element.

Ledning: $(a + b)^3 = a^3 + b^3$, $a, b \in K$. Visa att L har högst 9 element och minst 4 element.

KB 9 Sätt $\xi = \sqrt[3]{2}$, $\eta = \sqrt{2}$ och $\zeta = \sqrt[6]{2}$. Visa att

a) $Q(\xi,\eta) \subseteq Q(\zeta)$

b) $[Q(\xi):Q] = 3$ och $[Q(\xi,\eta):Q(\xi)] = 2$

c) $Q(\xi,\eta) = Q(\zeta)$.

KB 10 Antag att $[F(a):F] = p$, $[F(b):F] = q$ där $p \neq q$ är primtal. Visa att $[F(a,b):F] = pq$.

KB 11 Antag att grad (a) = n, grad (b) = m (över någon kropp F). Visa att grad (a + b) $\leq$ mn. Ge exempel på likhet.

KB 12 a) Antag, att f(b) = 0, f$\in$ K [X]. Visa att f är en multipel av det minimala polynomet till b.

b) Antag, att a, b$\in$ K$\supset$F är sådana att f(a) = 0$\Longrightarrow$f(b) = 0 för f$\in$ F[X]. Visa att man har en ringisomorfism F(a) $\overset{h}{\to}$ F(b) s.a. h(a) = b.

KB 13 Visa att Q(cos θ) är algebraisk över Q(cos 3θ). Vilka värden kan [Q(cos θ): Q(cos 3θ)] anta?

KB 14 Betrakta polynomet $f(X) = X^3 + X + 1 \in Q[X]$. Bestäm graden över Q för en rotkropp till f(X) över Q. (Man får utan bevis använda det faktum att f(X) har en unik reell rot.)

KB 15 a) Visa att polynomet $X^2 + 1$ är irreducibelt (= primpolynom) över Z_3.

b) Utvidga Z_3 till en kropp K där polynomet har rötter. Skriv upp alla elementen i denna kropp och ange vilka som är rötter till polynomet.

c) Visa att den multiplikativa gruppen av från 0 skilda element i K är cyklisk.

KB 16 Bestäm graden av en rotkropp till följande polynom över Q:
$X^4 - 2X^2 + 1$, $X^4 - X^2 + 1$, $X^4 + X^2 + 1$.

KB 17 Låt K vara rotkroppen till polynomet $X^4 + 3X^2 - 1$ i Q[X]. Beräkna [K:Q].

KB 18 Sök graden för en rotkropp till polynomet $X^p - 1$ över Q där p är ett primtal.

KB 19 Låt α vara en rot till $X^4 + X^2 = 1$. Sök graden för en rotkropp till $f = X^4 + 2X^2 (1 - 2\alpha^2) + 1$ över $Q(\alpha)$.

Ledning: Skriv f på formen $(X^2 + AX + 1)(X^2 + BX + 1)$.

KB 20 Låt K vara kroppen Z_2 av heltalen modulo 2. Visa att $f(X) = X^3 + X + 1$ är ett primpolynom i $K[X]$. Adjungera ett nollställe ξ till f. Ange antalet element i den utvidgade kroppen $K(\xi)$. Skriv upp alla elementen i $K(\xi)$ och undersök vilka av dem som är nollställen till f. Är $K(\xi)$ en rotkropp till f?

KB 21 Låt α, β, γ vara element i en utvidgning av den rationella talkroppen Q sådana att $x^3 - 5 = (x - \alpha)(x - \beta)(x - \gamma)$.

a) Vilket värde har graden $[Q(\alpha):Q]$? Ge en kort motivering.

b) Visa att β/α uppfyller ekvationen $x^2 + x + 1 = 0$.

c) Visa att $Q(\alpha) \cap Q(\beta) = Q$ och att $Q(\alpha + \beta) \neq Q(\alpha, \beta)$.

KB 22 $[F(a):F] = m$, $[F(b):F] = n$.

a) Visa att a har graden m över F(b) omm b har graden n över F(a).

b) Visa att i så fall gäller $F(a) \cap F(b) = F$.

KC 1 Visa att om K är en ändlig kropp så finns ett irreducibelt polynom (och alltså oändligt många) av grad ≥ 2 i $K[X]$.

KC 2 Låt F vara en kropp av karaktäristik $p > 0$. Visa att $\{x \in F \mid x^p = x\}$ utgör en delkropp $\cong Z_p$, den s.k. primkroppen i F.

KC 3 Bevisa att om en ändlig kropp K har q element så gäller $a^q = a$ för alla a i K. Visa att om $q > 2$ så är summan av elementen i K noll.

KC 4 Låt talet ξ vara algebraiskt av graden n över F, $n > 1$. Sätt $\eta = \frac{a\xi + b}{c\xi + d}$, där $a, b, c, d \in F$ och $ad \neq bc$.
Bevisa att $F(\xi) = F(\eta)$. Vilken grad har η över F?

KC 5 Antag att elementet $\alpha \neq 0$ tillhör en algebraisk kroppsutvidgning av den rationella talkroppen Q. Sätt $\beta = \alpha + \alpha^{-1}$.

a) Visa att $[Q(\beta):Q]$ är lika med antingen $[Q(\alpha):Q]$ eller $\frac{1}{2}[Q(\alpha):Q]$.

b) Kan båda möjligheterna inträffa?

KC 6 Låt L vara en delkropp av K(X), kroppen av rationella funktioner i variabeln X över K och antag L omfattar K strikt. Visa att $[K(X):L] < \infty$.

KC 7 $K \subset T \subset L$ K,L kroppar, T ring, L algebraisk över K. Visa att T är en kropp.

KC 8 Låt $F = Q(\sqrt{2}, \sqrt{3})$. Bestäm alla $u \in F$ med $F = Q(u)$. (Så kallade primitiva element.)

KC 9 Antag att $L = K(u,v)$, $[L:K] = p^2$, karaktäristiken för $K = p$ samt att $u^p, v^p \in K$. Visa att L/K saknar primitivt element, dvs. att $K(w) \neq L$, $\forall w \in L$.

KC 10 Bestäm graden för en rotkropp till $Z^3 - X^3$ över $K(X^3)$ för olika K.

KC 11 Bestäm graden för en rotkropp till $X^p - X - a$ över F, där F har karaktäristik p.

KC 12 Låt K vara en algebraisk utvidgning av F_0 och låt F_1 och F_2 vara delkroppar av K som omfattar F_0. F_1 och F_2 säges vara <u>lineärt åtskilda</u> över F_0 om $\forall x_1,\ldots,x_n$ lineärt oberoende element i F_1 över F_0 och $\forall y_1,\ldots,y_m$ lineärt oberoende element i F_2 över F_0 gäller att elementen x_iy_j $i = 1,\ldots,n$, $j = 1,\ldots,m$ är lineärt oberoende över F_0.

a) Om F_1 och F_2 är lineärt åtskilda över F_0, visa att $[F_1 \cup F_2 : F_1] = [F_2 : F_0]$ där $F_1 \cup F_2$ är den minsta delkropp av K som innehåller både F_1 och F_2.

b) Visa också att $F_1 \cap F_2 = F_0$.

c) Om x,y rötter till samma irreducibla polynom i $F_0[x]$ visa att $F_0(x)$ och $F_0(y)$ inte är lineärt åtskilda över F_0.

KC 13 Låt y vara en icke-reell rot till $x^3 = 2$. Visa att $\mathbb{Q}(\sqrt[3]{2}) \cap \mathbb{Q}(y) = \mathbb{Q}$ (så detta villkor är inte tillräckligt för lineär åtskildhet.)

Svar

KA 4 2, ∞, 6, 2

KA 6 $[K:Q] = 4$

KA 7 2

KA 8 6

KA 10 a) $\frac{1}{3}(1 - \sqrt[3]{2} + \sqrt[3]{4})$ b) $\frac{1}{2}(\sqrt{2} + \sqrt{3})^3 - \frac{9}{2}(\sqrt{2} + \sqrt{3})$

KA 11 a) 3, 4

b) 4, 2, 8, 2

c) 2

KA 13 b) 3 c) 4

KA 14 $x^2 + x + 1$, $x^2 + 1$, $x^4 + x^3 + x^2 + x + 1$, $x^2 - x + 1$

För R samma utom för n = 5 då man i stället får minimala polynomet

$x^2 + \frac{1 - \sqrt{5}}{2} x + 1$

KA 15 6, 12

KA 17 grad = 1 för p = 5, 17 , = 2 för p = 3, 11

KA 18 p = 3. Graden kan vara = 1 eller = 2

p = 5. Graden = 3

KA 20 b) 6

KA 21 2, 4, 4, 8, 4

KA 22 12

KA 23 a) 2 över Z_3 och R och 6 över Q

b) 4 över Q, 2 över R, 1 över Z_5

KA 24 1 eller 2. Som rotkropp duger R eller C.

Svar

KB 2 6 utgör enhetselementet

KB 4 a) 4 b) t.ex. $\gamma = i + \sqrt{3}$

KB 7 2 eller 3

KB 11 Exempelvis $a = \sqrt{2}$, $b = \sqrt{3}$ $F = Q$

KB 13 1, 2 eller 3

KB 14 6

KB 15 b)$K = \{ a + b\xi \mid a,b \in Z_3 \}$. Av dessa är ξ och 2ξ rötter till $X^2 + 1$.

KB 16 1, 4, 2

KB 17 8

KB 18 $p - 1$

KB 19 2

KB 20 ξ, ξ^2, $\xi + \xi^2$. Ja

KB 21 a) 3

Svar

KC 4 n

KC 5 b) Ja

KC 8 $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ åtminstone 2 av b, c, d $\neq 0$

KC 10 3 om $X^2 + X + 1$ har rot i K.

6 annars

KC 11 1 om $X^p - X - a$ har rot i K.

p annars

Ledningar

KA 2 En kropp har inga ideal $\neq 0, \neq K$.

KA 6 Visa att $K \cong Q(\sqrt{2},\sqrt{3})$

KA 7 $x^4 + x^3 + x^2 + x + 1 = (x^5 - 1)/(x - 1)$ dvs. dess rötter är de 5.e enhetsrötterna $\neq 1$.

KA 9 Använd trigonometriska formeln $\cos^2 \frac{\alpha}{2} = \frac{\cos \alpha + 1}{2}$

KA 10 a) $(\sqrt[3]{2} + 1)^{-1} \in K(\sqrt[3]{2})$. Ansätt.

b) $\sqrt{2} \in K(\sqrt{2} + \sqrt{3}) = K(\sqrt{2},\sqrt{3})$. Ansätt.

KA 14 En n:te enhetsrot är rot till $x^n = 1$. Sök den irreducibla faktor som har den primitiva n:te enhetsroten $e^{2\pi i/n}$ som rot.

KA 18 Om ett 3:e gradspolynom inte irreducibelt så har det en rot i grundkroppen. Undersök varje p för sig.

KA 19 b) Om K har q element och $[F:K] = n$ så har F q^n element.

KA 23 b) $x^4 + x^3 + x^2 + x + 1 = (x^5 - 1)/(x- 1)$

KA 24 Varje polynom av pos. grad i $C[X]$ kan skrivas som en produkt av lineära faktorer.

Ledningar

KB 1 Visa att F måste ha karaktäristik > 0. Då utgör multiplerna av enhetselementet en delkropp med p element.

KB 3 $[K(a):K] \mid [F:K]$

KB 6 Vilka möjligheter finns för $[F(a):F(a^2)]$?

KB 8 b) Vilken grad måste en sådan kropp ha över Z_3?

KB 10 Visa att $[F(a,b):F] \leq pq$.

Visa att både p och q delar $[F(a,b):F]$.

KB 12 a) Euklides algoritm

b) Visa att a och b har samma minimala polynom

KB 13 Anv. $\cos(\alpha + \beta) = \cos\alpha \cos\beta - \sin\alpha \sin\beta$ upprepade gånger.

KB 14 Om α reell rot till f så ligger $Q(\alpha) \subset R$ och kan inte innehålla någon komplex rot.

KB 15 c) Hitta element med maximal ordning genom att pröva.

KB 18 Visa att $Q(\xi)$, ξ primitiv p:te rot duger.

KB 21 b) Använd att $x^2 + x + 1 = (x^3 - 1)/(x - 1)$

samt att $\alpha^3 = \beta^3 = 5$

c) $\alpha + \beta + \gamma = 0$

Ledningar

KC 1 Betrakta polynomet $\prod_{a \in K} (X - a)$

KC 3 Betrakta den multiplikativa gruppen K^*

KC 5 Vilka värden kan $[Q(\alpha):Q(\beta)]$ anta?

KC 6 Visa att X är algebraiskt över L

KC 7 Visa att a^{-1} kan uttryckas som ett polynom i a.

KC 8 Ansätt $u = a\sqrt{2} + b\sqrt{3} + c\sqrt{6}$ och bestäm villkor på a,b,c så att u har grad ≤ 2 över Q.

KC 9 Visa att $w^p \in K \quad \forall w \in L$

KC 10 Visa först att $Z^3 - X^3$ är irreducibelt över $K(X^3)$. Adjungera sedan X, dividera med Z - X och studera eventuella rötter till kvoten i K(X).

KC 11 Tänk på rötterna till $X^p - X$.

Lösningar

KA 1 Enklast observeras att nZ är ett maximalt ideal omm n är ett primtal (≥ 2). Alternativt visas lätt att Z_n saknar nolldelare $\neq 0$ omm n är ett primtal och Lemma 3.2 sid. 90 kan användas.

KA 2 Ker f är ett ideal i K och $\neq$ K ty f $\neq 0$. $\therefore$ Ker f = 0.

KA 3 $(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}$ och om $0 < k < p$ är binomialkoefficienten $\binom{p}{k}$ delbar med p så motsvarande term = 0 och kvar blir $a^p + b^p$. Eftersom även $(ab)^p = a^p \cdot b^p$ följer att $a \to a^p$ definierar en ringhomomorfism $\neq 0$. Enligt KA 2 är den då 1 - 1.

KA 7 Man observerar att $x^4 + x^3 + x^2 + x + 1 = (x^2 + \frac{1+\sqrt{5}}{2} x + 1)(x^2 + \frac{(1-\sqrt{5})x}{2} + 1)$ där faktorerna är irreducibla i $Q(\sqrt{5})$ ty deras rötter är icke-reella.

KA 8 $\sqrt[3]{2} - \sqrt{5} \in Q(\sqrt[3]{2}, \sqrt{5})$ vars grad över Q är = 6 (adjunktion av $\sqrt[3]{2}$, rot till irreducibla $x^3 = 2$ och sedan adjunktion av $\sqrt{5}$ rot till irreducibla $x^2 = 5$). $\therefore$ grad $\sqrt[3]{2} - \sqrt{5}$ över Q = 1, 2, 3 el. 6. De 3 första alternativen elimineras genom ansättning och användande att $1, \sqrt[3]{2}, \sqrt[3]{4}, \sqrt{5}, \sqrt{5}\sqrt[3]{2}$ och $\sqrt{5}\sqrt[3]{4}$ är lin. ober. över Q.

KA 9 $\cos^2 \pi/12 = \frac{1}{2}(\cos \pi/6 + 1) = \frac{1}{2}(\sqrt{3}/2 + 1)$

KA 10 a) Ansätt $(\sqrt[3]{2} + 1)(A + B\sqrt[3]{2} + C\sqrt[3]{4}) = 1$ ger $A = C = \frac{1}{3}$ $B = -\frac{1}{3}$

b) Ansätt $2 = A(\sqrt{2} + \sqrt{3})^3 + B(\sqrt{2} + \sqrt{3})^2 + C(\sqrt{2} + \sqrt{3}) + D$ och använd att $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ lineärt oberoende över Q. Ger $11A + C = 1$ $9A + C = 0$ $B = D = 0$

KA 11 a) $\sqrt[3]{3} \cdot \sqrt[6]{4} = \sqrt[3]{6}$ rot till irreducibla $x^3 = 6$. Observera att $Q((\sqrt{2} + \sqrt{3})^{-1}) = Q(\sqrt{2} + \sqrt{3})$. Man eliminerar lätt möjligheten att graden = 2.

forts. lösningar

KA 11 b) $Q(\sqrt[4]{2}, \sqrt{2}) = Q(\sqrt[4]{2})$ och $x^4 - 2$ irreducibel, $\sqrt[4]{2}$ rot till irreducibla $x^2 = \sqrt{2}$ i $Q(\sqrt{2})[x]$. $Q(\sqrt[4]{2}, i\sqrt{2}) = Q(\sqrt[4]{2}, i)$ och $x^2 + 1$ irreducibel i $Q(\sqrt[4]{2})$. $Q(\sqrt{2}, \cos \pi/4) = Q(\sqrt{2})$

c) X rot till irreducibla $Z^2 - (X^2 + 1) + 1$

KA 12 a) grad b = $[F(b):F] = [F(a):F] = n$

b) Klart ur a) ty $F(a) = F(a^{-1})$

KA 13 b) $2^{2/3}$ rot till irreducibla $x^3 = 4$

c) $(\sqrt{2} - 1)^{1/2}$ rot till irreducibla $x^2 - \sqrt{2} + 1 \in Q(\sqrt{2})[x]$

KA 14 n = 3 $(x^3 - 1)/(x - 1) = x^2 + x + 1$

n = 4 $(x^4 - 1)/(x - 1)(x + 1) = x^2 + 1$

n = 5 $(x^5 - 1)/(x - 1) = x^4 + x^3 + x^2 + x + 1$

n = 6 $(x^6 - 1)/(x^3 - 1)(x + 1) = x^2 - x + 1$

För grundkroppen R se KA 7.

KA 15 $i\sqrt{6}$ är av grad ≤ 2 över $Q(\sqrt[3]{6})$ eftersom det är rot till polynomet $x^2 + 6$. Graden kan dock inte vara 1 ty $Q(\sqrt[3]{6})$ innehåller bara reella tal. Alltså är $[Q(\sqrt[3]{6}, i\sqrt{6}):Q] = 3 \cdot 2 = 6$.

$\sqrt{6}$ är av grad 2 över Q. Enligt sats 5A s. 168 så kan $\sqrt{6}$ då inte vara innehållet i $Q(\sqrt[3]{6})$ som är av grad 3 över Q. Man får $[Q(\sqrt[3]{6}, \sqrt{6}):Q] = 6$ och $[Q(\sqrt[3]{6}, \sqrt{6}, i):Q] = 6 \cdot 2 = 12$.

KA 16 $\alpha = 1 + \sqrt[5]{2} + 3\sqrt[5]{8} \in Q(\sqrt[5]{2})$ vars grad över Q = 5 så $1, \alpha, \alpha^2, \alpha^3, \alpha^4$ är lineärt oberoende över Q vilket ger det önskade polynomet.

KA 17 Graden = 1 eller 2 beroende på om $x^2 + 1$ har rot i Z_p eller ej. Prövning visar att rot i Z_p finns för p = 5 och p = 17 men ej för p = 3, p = 11.

KA 18 $x^3 + x^2 + 1$ irreducibelt över Z_5 inses gm prövning $\therefore [Z_5(\alpha):Z_5] = 3$

Över Z_3 har $x^3 + x^2 + 1$ roten 1 och $x^3 + x^2 + 1 = (x - 1)(x^2 + 2x + 2)$

där $x^2 + 2x + 2$ är irreducibelt över Z_3 så graden = 1 eller = 2 beroende på om $\alpha = 1$ eller ej.

KA 19 a) visas genom prövning.

b) Adjungera en rot α till f och sätt $K = Z_3(\alpha)$. $[K:Z_3] = 3$ så K har $3^3 = 27$ element.

KA 20 b) $K = Q(\sqrt[3]{2}, \varepsilon\sqrt[3]{2}, \varepsilon^2\sqrt[3]{2}) = Q(\sqrt[3]{2},\varepsilon)$ där ε är en primitiv 3:e enhets rot.

$[K:Q] = 6$, ty $[Q(\sqrt[3]{2},\varepsilon):Q(\sqrt[3]{2})] = 2$ och $[Q(\sqrt[3]{2}):Q] = 3$.

KA 21 $x^4 - 1 = (x + 1)(x - 1)(x^2 + 1)$

Så $K = Q(i)$ är en rotkropp och $[K:Q] = 2$

$x^4 + 1 = (x^2 + i)(x^2 - i)$ så $K = Q(i,\sqrt{i}) = Q(\alpha)$ $\alpha = e^{\pi i/4}$

så $[K:Q] = 4$

$x^6 + 1 = (x - \beta)(x - \beta^3)(x - \beta^5)(x - \beta^7)(x - \beta^9)(x - \beta^{11})$

där $\beta = e^{\pi i/6}$ så $K = Q(\beta)$ är en rotkropp med grad = 4 över Q

$x^4 + 2 = (x - \sqrt[4]{2}\xi)(x - \sqrt[4]{2}\xi^3)(x - \sqrt[4]{2}\xi^5)(x - \sqrt[4]{2}\xi^7)$

där $\xi = e^{\pi i/4}$ så $K = Q(\sqrt[4]{2},\xi)$ är en rotkropp med $[K:Q] = 8$

$x^5 - 1 = (x - 1)(x - \alpha)(x - \alpha^2)(x - \alpha^3)(x - \alpha^4)$

med $\alpha = e^{2\pi i/5}$, så $K = Q(\alpha)$ rotkropp och $[K:Q] = 4$

KA 22 Rotkroppen är $Q(\sqrt[6]{3},\varepsilon)$, där ε är en primitiv 6:e enhetsrot (t.ex.

$\varepsilon = e^{\pi i/3} = 1/2(1 + i\sqrt{3})$)

$Q(\sqrt[6]{3},\varepsilon) = Q(\sqrt[6]{3}, i\sqrt{3})$ vilket ger $[Q(\sqrt[6]{3},\varepsilon):Q] = 2 \cdot 6 = 12$

KA 23 a) $x^4 + x^3 + x^2 + x + 1 = (x^5 - 1)/(x - 1) =$

$(x^2 + \frac{1 + \sqrt{5}}{2} x + 1)(x^2 + \frac{1 - \sqrt{5}}{2} x + 1)$ där faktorerna är irreducibla i $R[x]$. (ty rötterna är icke-reella). Nu följer att $x^4 + x^3 + x^2 + x + 1$ är irreducibelt i $Q[x]$ ty saknar rationella rötter och om faktorisering i 2.a-gradsfaktorer existerar så nödvändigtvis lika med ovanstående ty

forts. lösningar

KA 23 a) forts.

R(x) har entydig faktoruppdelning. Slutligen över Z_5 har man

$x^5 - 1 = (x - 1)^5$ så $x^4 + x^3 + x^2 + x + 1 = (x - 1)^4$

KB 1 1, 1 + 1, ... kan inte alla vara olika så $n \cdot 1 = 0$ ngt n och minsta sådant n måste vara ett primtal, vilket just är karaktäristiken för K. Nu är $\underbrace{1 + \ldots + 1}_{k\text{st}} \to k \pmod p$ en isomorfism av ringar mellan $\{0, 1, \ldots, p-1\}$ och Z_p. Låt $n = [K:Z_p]$. Då har K p^n element.

KB 2 $6 \cdot 6 = 36 \equiv 6 \pmod{10}$. Man kan direkt kontrollera att alla element har invers (eller vilket också räcker att ringen saknar nolldelare). Ringaxiomen följer från motsvarande i Z.

KB 3 $[F:K] = [F:K(a)][K(a):K]$ och eftersom $[F:K] = p$ är primt så måste $[K(a):K] = 1$ eller $= p$, det senare ekvivalent med att $a \notin K$.

KB 4 a) $[Q(i,\sqrt{3}):Q] = 4$; adjungera först $\sqrt{3}$ och sedan i.

b) $\gamma = i + \sqrt{3}$ duger, ty $Q(i + \sqrt{3}) \subset Q(i,\sqrt{3})$ och de har samma grad över Q.

KB 5 a) Visa att ξ satisfierar en ekvation av grad 6 över Q, men att ξ ej är rationell.

b) Visa att n är delbart med både 2 och 3.

KB 6 $[F(a):F(a^2)] = 1$ eller 2 ty a alltid rot till $X^2 = a^2$. Om nu $[F(a):F]$ udda så är $[F(a):F(a^2)] = 1$ nödvändigt.

KB 7 Skriv $x^5 + x + 1 = (x^3 + x^2 + 1)(x^2 + x + 1)$ där båda faktorerna är irreducibla över Z_2 vilket inses genom prövning.

KB 8 a) $f(x) = x^4 + x^3 + x^2 + 1$ saknar 1:a gradsfaktor. (Pröva.) Ansätt $x^4 + x^3 + x^2 + 1 = (x^2 + Ax + B)(x^2 + Cx + D)$ och försök lösa för A, B, C, $D \in Z_3$ ger motsägelse. Adjungera nu rot α till f. Då har $K = Z_3(\alpha)$ $3^4 = 81$ element.

b) Om F delkropp av K så $[F:Z_3]$ delar $[K:Z_3] = 4$ dvs. $[F:Z_3] = 1$, 2 el. 4.

c) Ekvationen $x^9 - x = 0$ har högst 9 lösningar. Hela $Z_3 \subset L$ ty i Z_3 har man redan $a^3 = a$.

KB 9 a) $\xi = \zeta^2 \quad \eta = \zeta^3$

b) $X^3 - 2$ irreducibelt i $Q[X]$. $X^2 - 2$ irreducibelt över $Q(\xi)$.

c) $[Q(\xi,\eta):Q] = 2 \cdot 3 = 6$ enl. b)

Men $[Q(\zeta):Q] = 6$ också vilket visar likheten.

KB 10 Man har $[F(a,b):F] = [F(a,b):F(b)][F(b):F] \leq pq$

$[F(a,b):F] = [F(a,b):F(b)][F(b):F] = [F(a,b):F(a)][F(a):F]$ vilket visar att både p och q delar $[F(a,b):F]$ som då måste vara $\geq pq$.

KB 11 $a \neq b \in F(a,b)$ och $[F(a,b):F] = [F(a,b):F(a)][F(a):F] \leq mn$.

KB 12 a) Euklides algoritm ger $f = qg + r$ där g är minimala polynomet till b och graden för r är strikt mindre än den för g eller $r = 0$. Sätt in $x = b$ ger $r(b) = 0 \Longrightarrow r = 0$.

b) Om f är det minimala polynomet till a så följer av a) och $f(b) = 0$ att f måste delas av det minimala polynomet till b. Men f är irreducibelt så likhet måste gälla. Nu kan Kor till Sats 5.1 s. 184 användas. Alternativt definierar $a \to b$, $k \to k \quad k \in F$ en ringhomomorfism $K(a) \to K(b)$ som är surjektiv och alltså 1 - 1. (Jmfr KA 2)

KB 13 Man har $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$ dvs. $\cos\theta$ är en rot till $4X^3 - 3X - \cos 3\theta = 0$. Om $\theta = 0$ så $\cos\theta = \cos 3\theta = 1$ dvs. graden = 1.
Om $\theta = \pi/6$ så $\cos\theta = \sqrt{3}/2$ och $\cos 3\theta = 0$, dvs. graden = 2.
Om $\theta = \pi/9$ så $\cos 3\theta = \frac{1}{2}$ och $\cos\theta$ är en rot till $4x^3 - 3x - 1/2$ som är irreducibelt över Q.

KB 14 f är irreducibelt i $Q[X]$; ty om f vore reducibelt, så hade $f(X)$ en rationell rot m/n med $m|1$ och $n|1$ vilket ger motsägelse. f har däremot en <u>reell</u> rot ξ eftersom f är av grad 3. (Denna reella rot är unik, ty $f'(X) = 3X^2 + 1 > 0$) $[Q(\xi):Q] = 3$ och $Q(\xi) \subset R$. $f(X) = (X - \xi)(X^2 + \alpha X + \beta)$ i $Q(\xi)[X]$
Andragradsfaktorn är irreducibel enligt ovan. Låt η vara en av dess rötter. Då är $Q(\xi,\eta)$ rotkropp till f och $[Q(\xi,\eta):Q] = 6$.

KB 15 a) Faktorsatsen $\Longrightarrow$ ett andragradspolynom är reducibelt över Z_3 omm det har nollställe i Z_3. Pröva:

X	0	1	2
X^2+1	1	2	2

. $X^2 + 1$ är alltså irreducibelt över Z_3.

b) Låt ξ vara nollställe till $X^2 + 1$.

$K = Z_3(\xi) = \{a + b\xi \mid a, b \in Z_3, \xi^2 = -1 = 2\} =$

$= \{0, 1, 2, \xi, 1 + \xi, 2 + \xi, 2\xi, 1 + 2\xi, 2 + 2\xi\}$

ξ är förstås nollställe till $X^2 + 1$ men också $\underline{2\xi}$, ty

$(2\xi)^2 + 1 = 4\xi^2 + 1 = \xi^2 + 1 = 0$.

c) $K^* = K \setminus \{0\}$ är en grupp av ordning 8. K^* är cyklisk $\Longleftrightarrow$ det finns ett element av ordning 8 i K^*. ξ är av ordning 4. Pröva $1 + \xi$. Möjliga ordningar är 2, 4, 8 enligt Lagranges sats.

$(1 + \xi)^2 = 1 + 2\xi + \xi^2 = 2\xi \neq 1 \quad (1 + \xi)^4 = (2\xi)^2 = 4\xi^2 = 2 \neq 1$

$(1 + \xi)^8 = 2^2 = 1$. Alltså är $\sigma(1 + \xi) = 8$.

KB 16 $x^4 - 2x^2 + 1 = (x^2 - 1)^2 = (x - 1)^2(x + 1)^2$. Q är en rotkropp.

$x^4 - x^2 + 1 = 0$ ger $x^2 = \frac{1 \pm i\sqrt{3}}{2}$

Sätt $\alpha = \frac{1 + i\sqrt{3}}{2}$. Då är $\alpha^{-1} = \frac{1 - i\sqrt{3}}{2}$

Om nu $\beta = \frac{\sqrt{3} + i}{2}$ så $\beta^2 = \alpha$ och

$x^4 - x^2 + 1 = (x^2 - \alpha)(x^2 - \alpha^{-1}) = (x - \beta)(x + \beta)(x - \beta^{-1})(x + \beta^{-1})$

$\therefore K = Q(\beta) = Q(\sqrt{3} + i)$ är en rotkropp till $x^4 - x^2 + 1$ av grad 4.

$x^4 + x^2 + 1 = 0$ ger $x^2 = \frac{-1 \pm i\sqrt{3}}{2}$. Sätt $\alpha = \frac{-1 + i\sqrt{3}}{2}$.

Då är $\alpha^{-1} = \frac{-1 - i\sqrt{3}}{2}$. Om nu $\beta = \frac{1 + i\sqrt{3}}{2}$ så är $\beta^2 = \alpha$ och

$x^4 + x^2 + 1 = (x^2 - \alpha)(x^2 - \alpha^{-1}) = (x - \beta)(x + \beta)(x - \beta^{-1})(x + \beta^{-1})$

Så $F = Q(\beta) = Q(i\sqrt{3})$ är en rotkropp av graden 2.

KB 17 Påstår att $x^4 + 3x^2 - 1$ är irreducibelt i $\mathbb{Q}[x]$. Om polynomet har en förstagradsfaktor så måste det ha en rationell rot. En sådan måste vara 1 eller -1, vilka inte är rötter.

Den andra möjligheten är $x^4 + 3x^2 - 1 = (ax^2 + bx + c)(dx^2 + ex + f)$, där koefficienterna är rationella. Enligt Gauss lemma kan man anta att de är

Lösningar

KC 1 $1 + \prod_{a \in K} (X - a)$ är identiskt 1 på K. Har speciellt ingen rot. Tag irreducibel faktor.

KC 2 $X^p - X$ har högst p lösningar i en godt. kropp. Om K har karaktäristik p så är $n^p = (1 + \ldots + 1)^p = 1^p + \ldots + 1^p = n$, $n = 0,1 \ldots p-1$ så dessa utgör samtliga lösningar till $X^p - X$ och bildar en delkropp $\cong Z_p$ (jmfr KB 1)

KC 3 Multiplikativa gruppen i K ($= K^*$) har $q - 1$ element så ett godtyckligt element har en ordning som delar q. Speciellt är $a^{q-1} = 1$ vilket ger $a^q = a$ som också uppfylls av $a = 0$. Utveckla $\prod_{a \in K} (X - a)$. Man har $-\sum_{a \in K} a$ som koefficient för X^{q-1}. Men elementen i K är precis lösningarna till $X^q - X = 0$ så faktorteoremet ger $\prod_{a \in K} (X - a) = X^q - X$ och man ser att om $q \geq 3$ så är koefficienten för $X^{q-1} = 0$.

KC 4 $\eta \in F(\xi)$ och $\xi = \frac{b - \eta d}{\eta c - a}$ där nämnaren är $\neq 0$ p.g.a. villkoret $ad \neq bc$.
$\therefore \xi \in F(\eta)$ $\therefore F(\xi) = F(\eta)$ och därmed har automatiskt ξ samma grad över F som η nämligen n.

KC 5 a) Ekvivalent: Visa att α är av grad 1 eller 2 över $Q(\beta)$.
b) $\alpha = 1$, $\beta = 2$ ger $Q(\alpha) = Q(\beta)$; $\alpha = i$, $\beta = 0$ ger $[Q(\beta):Q] = \frac{1}{2}[Q(\alpha):Q]$.

KC 6 L innehåller element $f = p(X)/q(X)$ där p och q är relativt prima $\in K[X]$ och något av dem har positiv grad. Då är $q(Y) \cdot f - p(Y)$ ett polynom i $L[Y]$ som har X som rot så $[K(X):L] \leq \max$ (grad q, grad p).

KC 7 Att visa $a \in T \Longrightarrow a^{-1} \in T$.
Nu är $K(a) = K[a] \subset T$ ty T ring. Men $a^{-1} \in K(a)$ och ligger alltså i T.

KC 8 $u = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$. Bestäm a,b,c,d s.a. grad u = 1 eller 2 (i övriga fall blir u ett primitivt element). Man kan låta a = 0 (spelar ingen roll för graden av u).

Antag att $u^2 + Au + B = 0$. Man använder att $1,\sqrt{2},\sqrt{3}$ och $\sqrt{6}$ är lineärt oberoende över Q och identifierar koefficienter ger

$$\begin{cases} 6cd + Ab = 0 \\ 4bd + Ac = 0 \\ 2bc + Ad = 0 \\ 2b + 3c + 6d + B = 0 \end{cases}$$

vilket har rationell lösning b,c,d,A,B omm åtminstone två av b,c,d är = 0. $\therefore$ $u = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ har grad 4 över Q omm åtminstone 2 av b,c,d är $\neq 0$.

KC 9 Låt $w = \Sigma\, a_{ij} u^i v^j$ vara ett godtyckligt element i K(u,v). Då gäller $w^p = \Sigma\, a_{ij}^p\, u^{ip} v^{jp} \in K$ ty $u^p, v^p \in K$. Dvs $[K(w):K] \leq p \quad \forall\, w \in K(u,v)$.

KC 10 Man observerar först att $Z^3 - X^3$ är irreducibelt över $K(X^3)$. Ty om p/q vore en rot så $p^3 - X^3q^3 = 0$. p och q kan antas relativt prima så speciellt gäller att q delar 1 dvs q är en enhet och kan antas = 1. Om p har grad $k > 0$ så har p^3 graden 3k (i variabeln X^3) och alltså grad 9k i X vilket ger motsägelse.

Adjunktion av X ger en uppspaltning

$Z^3 - X^3 = (Z - X)(Z^2 + ZX + X^2)$ och frågan är när detta senare polynom är irreducibelt över K(X). Antag att p/q är en rot till $Z^2 + ZX + X^2$ ger $p^2 + p \cdot q \cdot X + X^2q^2 = 0$. p och q kan antas relativt prima så precis som ovan kan q = 1 antas. Då följer att p måste ha grad 1 och alltså formen aX + b. Insättning ovan ger $a^2 + a + 1 = 0$ $b = 0$, vilket också lätt ses vara tillräckligt för att aX skall vara en rot till $Z^2 + ZX + X^2$.

KC 11 Låt α vara en rot till $X^p - X - a$. Eftersom $k^p - k = 0$, $k = 0,\ldots,p-1$ följer att även $\alpha + k$ är rötter till $X^p - X - a$. Alltså är $F(\alpha)$ en rotkropp till $X^p - X - a = \prod_{k=0}^{p-1} (X - \alpha - k)$. Om nu $\alpha \notin F$ så måste $X^p - X - a$ vara irreducibelt ty en faktor måste vara en produkt av vissa $(X - \alpha - k)$ vars näst högsta koefficient $= -\Sigma(\alpha - k)$ som alltså $\in F$. Detta är nu bara möjligt om $\Sigma\alpha = 0$ dvs. α förekommer 0 eller p gånger.

KC 12 a) Antag att $y_1,\ldots,y_m \in F_2$ är lineärt oberoende över F_o. Det gäller att visa att de även är lineärt oberoende över F_1.

Antag $\sum_i a_i y_i = 0$ $a_i \in F_1$. Tag bas x_j för F_1 över F_o och skriv $a_i = \sum_j a_{ij} x_j$ $a_{ij} \in F_o$. Då gäller $\sum_{i,j} a_{ij} y_i x_j = 0$ och eftersom $y_i x_j$ är lineärt oberoende över F_o enligt förutsättningen om lineär åtskildhet, följer att alla $a_{ij} = 0$ dvs alla $a_i = 0$.

b) Det är klart att om $x \in F_1 \cap F_2 - F_o$ så är $1,x$ lineärt oberoende över F_o och då vore $1,x,x,x^2$ lineärt oberoende över F_o vilket uppenbarligen är orimligt.

c) Man har $[F_o(x):F_o] = [F_o(y):F_o] = n$ men över $F_o(x)$ har minimala polynomet till y grad $< n$ vilket visar $[F_o(x,y):F_o(x)] < [F_o(y):F_o]$ och man kan inte ha lineär åtskildhet enligt a).

KC 13 y komplex rot till $x^3 = 2$, säg $y = \sqrt[3]{2}\,(-\frac{1}{2} + \frac{i\sqrt{3}}{2})$. Elementen i $Q(y)$ har formen $ay^2 + by + c$. Antag något sådant $\in Q(\sqrt[3]{2}) - Q$. Då måste (1) a eller $b \neq 0$ och (2) $a = 0$ omöjligt ty by aldrig reellt för $b \in Q^*$. Visa att inte heller $ay^2 + by$ reellt för $a \neq 0$. $a = 1$ kan antas.

$y^2 + by = \frac{1}{4}\sqrt[3]{4}\,(1 - 3 - 2i\sqrt{3}) + \frac{b}{2}(-1 + i\sqrt{3})\sqrt[3]{2}$ är reellt omm $-\sqrt[3]{4} + b\sqrt[3]{2} = 0$ vilket är omöjligt för $b \in Q$.