

Inga hjälpmedel tillåtna. Motivering krävs i varje uppgift. Minst 15 poäng krävs för godkänt. Bonuspoäng från kontrollskrivningar kan användas för att tillgodoräkna deluppgifter från Uppgift 1 enligt följande. Du får själv välja vilka deluppgifter du vill tillgodoräkna: ange i förekommande fall dessa.

24-30 p 3 deluppgifter
 16-23 p 2 deluppgifter
 8-15 p 1 deluppgift

1. (a) Hur många inverterbara element finns det i ringen $\mathbb{Z}_{64}$? (1p)
- (b) Ange två grupper av ordning 4 som inte är isomorfa som grupper. (1p)
- (c) Finns det en graf som har fyra hörn, sex kanter och kromatiskt tal lika med 3? (1p)

Lösningförslag: (a) Antalet inverterbara element i $\mathbb{Z}_n$ ges av Eulers ϕ -funktion. Vi påminner oss att om p är ett primtal och $k \in \mathbb{N}$ så gäller $\phi(p^k) = p^k - p^{k-1}$. Detta ger

$$\varphi(64) = \varphi(2^6) = 64 - 32 = 32.$$

(b) Låt $G_1 = \mathbb{Z}_4$ med addition modulo 4 och låt $G_2 = V_4$, Kleins 4-grupp.

(c) Det existerar i själva verket precis en graf upp till isomorfi som har fyra hörn och sex kanter: den kompletta grafen K_4 . Denna har emellertid kromatiskt tal lika med 4, vilket ger att svaret på frågan är nej.

2. (a) Ge definition av tecknet för en permutation. Ge definitionen av den alternerande gruppen av ordning n . (2p)
- (b) Skriv permutationerna $\alpha, \beta \in S_8$ som ges av

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 4 & 2 & 8 & 7 & 6 & 5 \end{pmatrix} \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 4 & 3 & 7 & 8 & 6 & 5 \end{pmatrix}$$

på cykelform. (2p)

- (c) Beräkna tecknet för α och β . Tillhör α och β den alternerande gruppen A_8 ? (2p)

Lösningförslag:

(a) Tecknet för en permutation σ ges av $(-1)^N$ där N är antalet transpositioner i någon framställning av σ som produkt av transpositioner. Den alternerande gruppen A_n består av de permutationer i den symmetriska gruppen S_n som är jämna.

(b) Vi ser att α fixerar 1 och att $2 \rightarrow 3 \rightarrow 4$ så att α innehåller cykeln (234). Permutationen α transponerar vidare 5 och 8 samt 6 och 7. Detta ger oss

$$\alpha = (234)(58)(67).$$

På liknande sätt ser vi att β innehåller transpositionerna (12) och (34) samt 4-cykeln (5768)

$$\beta = (12)(34)(5768).$$

(c) För att beräkna tecknet hos α skriver vi om tre-cykeln $(234) = (23)(34)$ och får nu $\alpha = (23)(34)(58)(67)$ vilket ger att α är en jämn permutation. Vi har vidare att

$$(5768) = (58)(56)(57)$$

vilket ger vid handen att β är en udda permutation. Därmed tillhör α den alternerande gruppen A_8 medan β ej är element i A_8 .

3. (a) Låt p vara ett primtal. Visa att villkoret $f(0) - g(0) = 0$ definierar en ekvivalensrelation på polynomringen $\mathbb{Z}_p[x]$. (2p)
- (b) Hur många ekvivalensklasser finns det? (1p)
- (c) Visa att mängden av ekvivalensklasser kan ges strukturen av en kropp. (2p)

Lösningsförslag:

(a) Villkoret $f(0) - g(0) = 0$ är ekvivalent med att konstantertermerna i polynomen f och g är lika. Vi identifierar alltså polynom som har samma konstantertermer, vilka är element i $\mathbb{Z}_p$. Att relationen är en ekvivalensrelation följer nu från aritmetik i $\mathbb{Z}_p$.

(b) Det finns enligt ovan precis p ekvivalensklasser.

(c) Detta följer av det kända faktumet att $\mathbb{Z}_p$ är en kropp.

4. (a) Bestäm antalet polynom i $\mathbb{Z}_5[x]$ av grad 4 som uppfyller villkoren $f(2) \neq 0$ och $f(3) \neq 0$. (3p)
- (b) För vilka $a \in \mathbb{Z}_5$ är polynomet $x^3 + 2x + a$ irreducibelt i $\mathbb{Z}_5[x]$? (3p)

Lösningsförslag:

(a) Låt $f(x) = a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$. Att polynomet har grad 4 medför att $a_4 \in \{1, 2, 3, 4\}$. Det finns totalt 2500 sådana polynom. Om $f(2) = 0$ fås enligt faktorsatsen att $f(x) = (x - 2)(b_3x^3 + b_2x^2 + b_1x + b_0)$ där $b_3 \neq 0$. Det finns $4 \cdot 5^3$ sådana polynom. På samma sätt erhåller vi att det finns $4 \cdot 5^3$ polynom i $\mathbb{Z}_5[x]$ med $f(3) = 0$.

Om $f(2) = f(3) = 0$ har vi $f(x) = (x - 2)(x - 3)(c_2x^2 + c_1x + c_0)$ med $c_2 \neq 0$. Det finns $4 \cdot 5^2$ sådana polynom.

Enligt principen om inklusion/exklusion ges det totala antalet polynom med $f(2) \neq 0$ och $f(3) \neq 0$ av

$$4 \cdot 5^4 - 4 \cdot 5^3 - 4 \cdot 5^3 + 4 \cdot 5^2 = 4 \cdot 5^2 \cdot (5^2 - 2 \cdot 5 + 1) = 100 \cdot 16 = 1600.$$

(b) Det givna polynomet har grad 3. Enligt en känd sats är polynomet $f = x^3 + 2x + a$ irreducibelt precis när det saknar en rot i $\mathbb{Z}_5$. Vi undersöker för varje $a \in \{0, 1, 2, 3, 4\}$ huruvida rötter föreligger.

Fallet $a = 0$ är trivialt då vi kan skriva $x^3 + 2x = x(x^2 + 2)$. Polynomet är då ej irreducibelt.

Vi sätter $a = 1$ och beräknar $f(0) = 1$, $f(1) = 1 + 2 + 1 = 4$, $f(2) = 8 + 4 + 1 \equiv 3$, $f(3) = 27 + 6 + 1 \equiv 4$ samt $f(4) = 64 + 8 + 1 \equiv 3$. Polynomet saknar rot och är därmed irreducibelt.

När $a = 2$ har vi $f(1) = 1 + 2 + 2 \equiv 0$. Därmed har f en rot och är ej irreducibelt.

Låt $a = 3$ och observera att $f(2) = 8 + 4 + 3 \equiv 0$: återigen har f en rot och är ej irreducibelt.

Slutligen sätter vi $a = 4$ och använder räkningarna för $a = 1$ för att dra slutsatsen att $f(0) = 4$, $f(1) = 2$, $f(2) = 1$, $f(3) = 2$ samt $f(4) = 1$. Polynomet saknar rötter och är därmed irreducibelt.

5. (a) Betrakta gruppen D_4 som ges av symmetrier på en kvadrat med gruppoperationen sammansättning. Beskriv samtliga gruppelment och bestäm gruppens ordning. (2p).
- (b) Är D_4 en abelsk grupp? (1p)
- (c) Innehåller D_4 någon delgrupp av ordning 2? Innehåller D_4 någon delgrupp av ordning 4? (2p)

Lösningsförslag:

(a) Symmetrierna till en kvadrat ges av rotationer och speglingar, närmare bestämt rotation med 90, 180 och 270 grader och spegling i kvadratens sidor samt i kvadratens diagonaler.

Om r betecknar en rotation med 90 grader har vi $r^4 = \text{id}$. Låt s beteckna spegling genom en av linjerna. Vi inser att de tre återstående speglingarna nu kan skrivas som sammansättningar av r och s , närmare bestämt ger $\{\text{id}, r, r^2, r^3, s, sr, sr^2, sr^3\}$ en lista över samtliga grupp-element.

Gruppens ordning är 8.

(b) Gruppen D_8 är ej abelsk då exempelvis $rs \neq sr$.

(c) Delgruppen $\{\text{id}, r, r^2, r^3\}$ av rotationer har ordning 4. Eftersom $s^2 = \text{id}$ utgör $\{\text{id}, s\}$ en delgrupp av ordning 2

6. (a) Vad menas med en checkmatris hörande till en linjär kod i $(\mathbb{Z}_2)^5$? (1p)

(b) Hur definieras minimiavståndet för en linjär kod? Finns det en linjär kod i $(\mathbb{Z}_2)^5$ som har minimiavstånd 5? (2p)

(c) Utgör

$$C = \{(00000), (10101), (11010), (11110), (11111)\} \subset (\mathbb{Z}_2)^5$$

en linjär kod? (2p)

Lösningförslag:

(a) Se kursboken för en definition av checkmatris.

(b) Se kursboken för definition av minimiavståndet. Koden $C = \{(00000), (11111)\}$ har som synes minimiavstånd 5.

(c) En linjär kod är en delgrupp till $(\mathbb{Z}_2)^5$ och har således jämn ordning enligt Lagranges sats. Eftersom C innehåller fem element är C således ej en delgrupp.