MATEMATISKA INSTITUTIONEN
STOCKHOLMS UNIVERSITET
Avd. Matematik
Rikard Bøgvad

Algebra och kombinatorik VT 2024
Tentamen 20 augusti 2024

LÖSNINGSSKISS

1. G är den minsta delgrupp till S_4 som innehåller permutationerna (23) och (34).

   Observera att de två permutationerna bara involverar symbolerna $2, 3, 4$ och att därför $G \subset S_3$, där den sista ses som permutationer av $2, 3, 4$. Kom ihåg att S_3 har 6 element. Man kollar lätt att $\pi := (234) = (23)(34)$ så därför innehåller G åtminstone två involutioner och enhetselementet samt π och i^2, d v s 5 element. Med Lagranges sats, som säger att ordningen av G delar ordningen av S_3, d v s 6, så måste G vara hela symmetrigruppen på $2, 3, 4$. Detta ger svaret till a). (Ange ordningen av G och beskriv explicit alla element i G.) Delgrupper till G kan ha ordning 1,2,3,6, där ordning 1 svarar mot enhetslementet e sett som en delgrupp, och ordning 6 mot hela gruppen G. En delgrupp av ordning 2 innehåller bara ett element förutom e, och kvadraten på det elementet måste vara e. Det är alltså en involution och det finns bara tre sådana i symmetrigruppen på $2, 3, 4$, nämligen $(23), (24), (34)$, som alltså ger upphov till 3 delgrupper. En delgrupp av ordning 3 innehåller inga delgrupper(Lagranges teorem igen eftersom 3 är ett primtal) så om π är ett element i den måste de andra elementen vara e, π^2 samt $\pi^3 = e$. Då är π(och π^2) en 3-cykel och bildar tillsammans med e den unika delgruppen av ordning 3. Nu har vi beskrivit alla delgruppetr och svarat på b). Slutligen är den bijektiva grupphomorfin f med S_3, där den sista ses som permutationer av $1, 2, 3$ uppenbar: den ges av att en permutation av de tre objekten $2, 3, 4$ betraktas som en permutation av $1, 2, 3$, t ex $f((234)) = (123)$. Att det är en grupphomorfi d v s $f(\pi\sigma) = f(\pi)f(\sigma)$ mm är klart från denna tolkning.

2. Låt C vara koden $C := \{[7^k]_2,\ k = 1, 2, 3\}$, där $[x]_2$ står för det positiva heltalet x uttryckt binärt.

   a) Hur många fel detekterar respektive rättar C? 2 p

   Koden innehåller bara tre element, nämligen $[7]_2 = ..000111$ och $[7^2]_2 = ..0110001$ och $[7^3]_2 = ..0101010111$. Okulär inspektion

ger att dessa tre skiljer sig från varandra med minst 3 bitar, och alltså rättar koden (enligt kursmaterialet, avsnittet om Hammingavstånd) 1 fel och detekterar 2.

b) Antag att vi har en lösning till ekvationen $7^k - 7^l = \pm 2^m \pm 2^n$, där $m, n, k, l \in \mathbb{Z}$, samt $m > n$ och $k > l \geq 1$. Eftersom k, l är positiva heltal,så gäller att m, n också måste vara det. Uppenbarligen kan inte bägge potenserna av 2 tas med minustecken eftersom vänstersidan av ekvationen är positiv. Skriv alltså om ekvationen till

$$7^l(7^{k-l} - 1) = 2^n(2^{m-n} + \pm 1).$$

Följande ledningen och räknande modulo 7 ser vi att $2^{m-n} + \pm 1 \cong 0 \implies m - 1 \cong 0(mod 3)$ och framförallt att $2^{m-n} + \pm 1 = 2^{m-l} - 1$(ty med ett plustecken finns ingen lösning mod 7). Vi får vidare p g a unik primtalsfaktorisering att $7^l = 2^{m-n} - 1 \iff 7^l + 1 = 2^{m-n}$ och att $7^{k-l} - 1 = 2^n$. Multiplicera ihop de sista två ekvationerna och få $(7^l + 1)(7^{k-l} - 1) = 2^n \iff 7^k + 7^{k-l} - 7^l = 2^m + 1$. Vänsterledet här är delbart med 7, p g a villkoren på $k.l$, men inte högerledet enligt moduliräkningen nyss. Detta visar att det inte finns några sådana lösningar.

c) Vi ska alltså visa att elementen i $\tilde{C}$ skiljer sig åt med åtminstone 3 bitar. Antag motsatsen: om kodorden som hör till $7^k > 7^l$(där $l \geq 1$) skiljer sig bara på två bitar så gäller att $7^k - 7^l = 2^m \pm 2^n$. Enligt b) är detta inte möjligt. Alltså skiljer sig kodorden på åtminstone tre bitar och rättar alltså 1 fel.

3. Låt H vara en delgrupp till den ändliga gruppen G. Definiera två relationer $\cong_R$ och $\cong_L$ på G på följande sätt:

$$x \cong_R y \iff y^{-1}x \in H \qquad x \cong_L y \iff xy^{-1} \in H.$$

a) Visa att bägge relationerna är ekvivalensrelationer(det räcker att ge detaljer för den ena). Vi exemplifierar med symmetriegenskapen: om $x \cong_R y$ så är alltså $y^{-1}x \in H \implies (y^{-1}x)^{-1} \in H$ eftersom H är en delgrupp. Men $(y^{-1}x)^{-1} = x^{-1}y$, vilket innebär att $y \cong_R x$, enligt definitionen. På samma sätt följer de två andra egenskaperna hos en ekvivalensrelation ur $e \in H$ och av att H är sluten under multiplikation.

2p

b) Givet $x \in G$ är ekvivalensklassen till vilken x hör

$$\{y : y^{-1}x = h \in H\} = \{y : y = xh^{-1} \in H\} = \{xk,\ k \in H\} = xH.$$

c) Enligt b) är ekvivalensklasserna vänster respektive höger koset till H i G. Enligt Lagranges sats är antalet koset lika med indexet $|G|/|H| = 2$. H är både ett vänster och höger koset, så det andra (vänstra respektive högra)kosetet består precis av de element som INTE ingår i H. Alltså är det både ett vänster och höger koset. Därmed sammanfaller ekvivalensklasserna för de två relationerna, och då är förstås också de två ekvivalensrelationerna desamma. V.s.v.

4. a) Hur många olika grafer på 10 hörn $v_1, ...v_{10}$ finns det? Vi räknar grafer av den typ som studerats under kursen. En kant är alltså en delmängd $\{v, w\} \subset V$, där V står för vertexmängden. Det finns alltså $\binom{10}{2} = 45$ möjliga kanter. En graf är bestämd av vilka av dessa kanter den innehåller, alltså av en delmängd till en mängd med 45 element. Enligt en sats i boken finns det 2^{45} sådana delmängder och detta är alltså antalet grafer.

   b) Packa upp definitionerna, så är det mycket enkelt....

   c) Att en graf är regulär innebär att det går lika många kanter från varje hörn. Om det från ett hörn i en graf med 6 hörn går fem kanter så går de till samtliga de andra hörnen, och grafen har alltså en kant mellan varje par av hörn och är den fullständiga grafen på 6 hörn. En sådan har $\binom{6}{2} = 15$ kanter.

5. Låt G beteckna symmetrigruppen till en regelunden 6-hörning med hörnen $V = \{v_1, ..., v_6\}$. Observera att den har egenskapen att ta kanter till kanter och diagonaler till andra eller samma diagonal.

   a) Att vi har en gruppverkan följer (med lite arbete) direkt ur definitionen. Om (v, w) är två hörn som ligger bredvid varandra på 6-hörningen, kommer symmetrigruppen att kunna överföra motsvarande kant till vilken annan kant som helst(inklusive (w, v) genom spegling), men inte till någon diagonal i 6-hörningen. Dessa element (v, w) bildar alltså en bana, med 12 element. En annan består av

   $$\{(v_i, v_i)\ i = 1, 2, ..., 6\}$$

   med 6 element. Geometrin, att titta på diagonaler, ger att ytterligare en bana med 6 element består av de hörn som ligger mittemot varandra:

   $$\{(v_1, v_4), (v_2, v_5), (v_3, v_6), (v_4, v_1), (v_5, v_2), (v_6, v_3)\}.$$

Den sista banan svarar mot de diagonaler som inte är symmetriaxlar t ex (v_1, v_3) och har 12 element. Tillsammans är detta de 36 elementen i $V \times V$. Alltså finns det 4 banor.

b) G består av rotationerna e, r, r^2, r^3, r^4, r^5 och speglingar $s_1, s_2, ...s_6$ i de 6 symmetriaxlarna. En spegling med symmetriaxel genom v och w kommer att ha 2 fixpunkter, nämligen (v, v) och (w, w). Rotationerna $r, r^2, r^3.r^4, r^5$ bevarar inga element, medan e bevarar alla 36 elementen i $V \times V$. Burnsides ekvation ger alltså

$$\textit{antalet banor} = \frac{1}{12}(36 + 6 \cdot 2) = 4,$$

alltså samma resultat som vi fick nyss

6. Om ett tredjegradspolynom kan faktoriseras i två polynom av lägre grad måste åtminstone ett av dessa ha grad 1, och då har polynomet ett nollställe. Det finns bara tre element i Z_3, så det är lätt att leta efter nollställen, för ett polynom av typen $p(x) = x^3 + x^2 + ax + b$:

$$p(0) = b, \quad p(1) = 2 + a + b, \quad p(-1) = -a + b.$$

Genom att gå igenom samtliga nio möjligheter för a, b ser man att alla dessa polynomvärden är nollskiljda, och motsvarande polynom alltså irreducibelt, omm $(a, b) = (1, 1), (0, -1), (1, -1)$.