MATEMATISKA INSTITUTIONEN
STOCKHOLMS UNIVERSITET
Avd. Matematik
Examinator: Samuel Lundkvist

Algebra och kombinatorik VT 2024
Tentamen 22 maj 2024

Lösningar

1. a) Välj två element π, σ i G, som inte har några fixpunkter, och inte kommuterar och räkna på cykelform ut $\pi\sigma,\ \sigma\pi$ och π^{-1}.
   Tag t ex $\pi := (12)$ och $\sigma := (23)$. Då är $\pi\sigma = (123),\ \sigma\pi = (132)$ och $\pi^{-1} = \pi$.

   b) Det finns två banor, där den ena består av alla par (a, b) där $a \neq b$. Detta eftersom det finns en permutation i G som tar ett par (a, b) där $a \neq b$ till vilket annat par (c, d) där $c \neq d$ som helst. Den andra banan består av alla par (a, a) där de två koordinaterna är lika—det finns ju en permutation som tar ett sånt par till vilket som helst annat sådant par, och en permutation tar ett sådant par till ett annat sådant par.

   c) Enligt en sats i boken består konjugatklassen

   $$\{g^{-1}\tau g,\ g \in G\}$$

   av alla permutationer med samma cykelstruktur, d v s alla transpositioner. Så frågan är ekvivalent med att bestämma antalet transpositioner i G. En transposition $(ab) = (ba)$ är bestämd av mängden $\{a, b\}$, så svaret är $\binom{7}{2} = 21$.

   d) Observera först att $U(\mathbb{Z}) = \{-1, 1\}$, som är en grupp med operationen multiplikation av heltal. Enligt en känd sats, eller definitionen, är produkten av jämna permutationer jämn: produkten av en udda och en jämn en udda permutation; och produkten av två udda permutationer udda. Detta säger precis att $f(\pi\sigma) = f(\pi)f(\sigma)$...och alltså är f en grupphomomorfi. Det är klart att f är surjektiv: det säger ju bara att det finns både udda och jämna permutationer.

2.

a) Det finns 9 matriser av formen $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ eftersom a, b kan ta 3 värden var. Villkoret $a^2 + b^2 \neq 0$ utesluter endast $(a, b) = (0, 0)$(kollas lätt

genom prövning!), d v s nollmatrisen. Alltså $|G| = 8$. Nu behöver vi bara kolla gruppaxiomen(utom associativiteten, som vi inte ehöver kolla, och som f ö följer av att matrismultiplikation är associativ, även över andra kroppar än $\mathbb{R}$.) Först visar vi att produkten av två matriser i G tillhör G. Produkten

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac - bd & ad + bc \\ -bc - ad & -bd + ac. \end{pmatrix}$$

är ju verkligen av rätt form, och villkoret att elementen i matrisen inte är noll är också uppfyllt. Vidare innehålls enhetsmatrisen $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ i G, och inversen till $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ är $\frac{1}{a^2+b^2} \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$. (Det uttrycket hittar man t ex via Gausselimination.)

b) $|G| = 8$.

c) Räkna potenser på några slumpvis element i G. Att G är cyklisk innebär ju att det ska finnas ett element vars potenser ger hela G. Tag t ex $g = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$, och kolla att $g^2 = \begin{pmatrix} -1 & -1 \\ 1 & -1 \end{pmatrix}$, och att $g^4 = (g^2)^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \neq Id$. Eftersom Lagranges sats säger att ordningen av ett element delar gruppens ordning, är de möjliga ordningarna för g 1,2,4,8. Vi visade precis att ordningen inte är $1, 2, 4$ så då måste den vara 8, och gruppen är cyklisk med g som generator. Delgrupper kommer att vara

$$\{id\}, \{id, g^4\}, \{id, g^2, g^4, g^6\}, G.$$

(Det finns en allmän beskrivning av delgrupper till cykliska grupper, men man kan också bara tänka så här: Låt H vara en delgrupp, och titta på ett element g^k, $0 \leq k < 8$ i H, med minimalt k. Om $k = 1$ så är $g : s$ potenser $< g >$ hela G, om $k = 2$ får vi den andra gruppen i listan, om k=3 så är $g^9 = (g^3)^3 = g$ i H så $H = G$, o sv.)

3. Låt $A = \{R, G, B\}$ och A^6 alla strängar med 6 element ur A. På A^6 verkar rotationsgruppen $R = \{e, r, r^2, ..., r^5\}$ med en verkan som ges av $r \cdot x_1x_2x_3x_4x_5x_6 = x_6x_1x_2x_3x_4x_5$, etc.

a) Gå igenom gruppelementen i R: De enda element som sta biliserar strängen är e, r^2, r^4, och de utgör alltså stabilisatorn.

b) Fixpunkter till r^2 är de strängar $UVWXYZ$ som inte ändras om vi skjuter alla färger framåt två steg(cykliskt). Alltså måste $U = W = Y$ och $V = X = Z$, och dessa två färger kan väljas fritt. Alltså är svaret $3 \cdot 3 = 9$

c) Det finns 3^6 strängar och vi räknar nu ut fixpunkterna till de olika elementen i G. Elementet e fixerar alla 3^6, elementen r, r^5 fixerar 3 element(enfärgade strängar), elementen r^2, r^4 fixerar 9 element, och r^3 fixerar 27 strängar. Burnsides sats ger då att

$$\text{antalet banor} = \frac{3^6 + 2 \cdot 3^2 + 2 \cdot 3 + 3^3}{6}.$$

4. Hur många ord kan man bilda med alla bokstäverna i ordet GRUPPHOMOMORFI om orden GRUP,MOM och FI inte får förekomma som delord i ordet? (GURPPHOMMOORIF är alltså ok men inte GRUPPHOMMOORIF...) (5p) Kardinaliteten av den mängd X av ord man kan bilda av alla bokstäverna i ordet GRUPPHOMOMORFI ges av multinomialkoefficienten

$$\frac{14!}{1!2!1!2!1!3!2!1!1!}.$$

Kardinaliteten av den mängd A av ord man kan bilda av alla bokstäverna i ordet GRUPPHOMOMORFI som innehåller GRUP (som då betraktas som en enda bokstav)ges av multinomialkoefficienten

$$\frac{11!}{1!1!1!3!2!1!1!1!}.$$

Kardinaliteten av den mängd B av ord man kan bilda av alla bokstäverna i ordet GRUPPHOMOMORFI som innehåller MOM ges av multinomialkoefficienten

$$\frac{12!}{1!2!1!2!1!2!1!1!}.$$

Kardinaliteten av den mängd C av ord man kan bilda av alla bokstäverna i ordet GRUPPHOMOMORFI som innehåller MOM ges av

$$\frac{13!}{1!2!1!2!1!3!2!1!}.$$

Vidare

$$|A \cap B| = 9!/2!$$

$$|A \cap C| = 10!/(3!2!)$$
$$|C \cap B| = 11!/(2!2!2!)$$
$$|A \cap B \cap C| = 8!/2!.$$

Svaret kan nu fås med bokens formel för inklusion och exklusion.

5. a) En RSA-kod är baserad på talet $n = 65$. Den offentliga nyckeln är e=11, budskapet 2. Vad är det krypterade meddelandet? Vad är den privata nyckeln d?

   Budskapet 2 krypteras till $2^{11}(mod 65)$. Räknar man på potenser, ser man efter ett tag att $2^6 = 64 = -1(mod 65)$ och alltså är $2^{11} = -2^5 = 33(mod 65)$. Den privata nyckeln fås genom att man löser ekvationen $11d = 1(mod \phi(65)$. Det sker via en diofantisk ekvation och svaret är $d = 35$.

   b) En lineär kod har paritetscheckmatrisen $\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$.

   Hur många kodord finns det?

   Man kollar att de tre raderna i matrisen är lineärt oberoende. Löser man motsvarande ekvationssystem får man alltså $7 - 3 = 4$ parametrar, vilket ger $2^4 = 16$ kodord. Man kan också känna igen matrisen som den som hör till en Hammingkod beskriven i läroboken.

   Beräkna paritetscheckmatrisen H gånger meddelandet 0001011. Resultatet är (101) som man känner igen som den femte kolonnvektorn i H. Alltså är det korrekta meddelandet (under antagande av högst ett fel) 0001111.

6. a) Polynomet $p(x) := x^2 + x + 1 \in \mathbb{Z}_2[x]$ är irreducibelt om det inte är produkten av två lineära polynom, eftersom det har grad 2. Detta i sin tur är ekvivalent med att polynomet inte har några nollställen i $\mathbb{Z}_2$, vilket är lätt att verifiera är fallet.

   b) Definiera en relation $\equiv$ mellan polynom i $\mathbb{Z}_2[x]$ på följande sätt:

   $$r(x) \equiv s(x) \iff p(x)|(r(x) - s(x)).$$

   Att detta är en ekvivalensrelation följer av att vi packar upp vad de olika villkoren på en ekvivalensrelation betyder i detta fall. Vi visar två av dem:

$$r(x) \equiv r(x) \iff p(x)|(r(x) - r(x)) = 0,$$

$$(r(x) \equiv s(x) \iff s(x) \equiv r(x))$$

eftersom $p(x)|(r(x) - s(x)) \iff p(x)|(s(x) - r(x) = -(r(x) - s(x))$, o s v.

c) Låt $s(x)$ vara ett polynom och $r(x)$ resten av $q(x)$ vid division med $p(x)$. Då gäller att $s(x) - r(x) = k(x)p(x)$, d v s att $s(x) \equiv r(x)$. Det finns fyra möjliga polynom av grad mindre än 2 i $\mathbb{Z}_2[x]$: $0, 1, x, x + 1$, och alltså precis fyra ekvivalensklasser.

d) Titta på resterna i föregående uppgift: $1 \cdot 1 = 1$, och $x \cdot (x + 1) = x^2 + x = (x^2 + x + 1 + 1)$. Så för dessa tre nollskilda rester finns det ett $t(x)$ som i pro lemställningen. Ta nu ett godtyckligt polynom $s(x)$ s a $s(x) \not\equiv 0$(Det står fel i uppgiften, det är detta villkor som avses!!). Delas det med $p(x)$ fås $s(x) = k(x)p(x) + r(x)$. Polynomets rest $r(x)$ är en av de tre resterna ovan och det finns alltså ett $t(x)$ så att $p(x)|t(x) \cdot r(x) - 1 \iff 1 = t(x) \cdot r(x) + l(x)p(x)$. Det följer att

$$t(x)s(x) = t(x)k(x)p(x) + t(x)r(x) = 1 + (t(x)k(x) + l(x))p(x),$$

vilket säger att $t(x)s(x) - 1$ är en multipel av $p(x)$ eller $t(x)s(x) \equiv 1$.