MATEMATISKA INSTITUTIONEN
STOCKHOLMS UNIVERSITET
Avd. Matematik
Examinator: Samuel Lundkvist

Algebra och kombinatorik VT 2024
Tentamen 22 maj 2024

För godkänt är det tillräckligt med 15 av de 30 poängen, inklusive bonuspoäng. *Samtliga svar måste motiveras utförligt! Ange för säkerhets skull hur många bonuspoäng du har uppnått!* Lärare kommer att besöka tentasalarna efter ungefär halva tentamenstiden. Lycka till!

TENTAMEN

1. Elementen i gruppen $G = S_7$ verkar på $X = \{1, 2, 3, ...7\}$ som permutationer.

   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}. (1 p)

   b) G verkar också på $Y := X \times X$ genom $\pi(a, b) = (\pi(a), \pi(b))$ om $(a, b) \in Y$ och $\pi \in G$.(Det behöver inte visas). Beräkna antalet banor som denna verkan har och beskriv dem.
   Ledning: Använd INTE Burnsides lemma.... (1p)

   c) Transpositionen $\tau = (12) \in G$. Beräkna kardinaliteten av

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

   (Obs: Svaret får innehålla kombinatoriska uttryck av den typ som förekommit i kursen —fakulteter, binomialkoefficienter, etc—och dessa behöver inte räknas ut!) (1p)

   d) Definiera funktionen $f : G \to U(\mathbb{Z})$ genom $f(\pi) = 1$ om π är en jämn permuatation, och $f(\pi) = -1$ om π är en udda permuatation. Visa att f är en surjektiv grupphomorfi. Utgå från kända egenskaper för udda/jämna permutationer— dessa behövs alltså inte visas. (2p).

2. Låt

   $$G := \{\begin{pmatrix} a & b \\ -b & a \end{pmatrix},\ a, b \in \mathbb{Z}_3,\ a^2 + b^2 \neq 0\}.$$

   a) Visa att G är en grupp med matrismultiplikation som gruppoperation(Associativitet behöver inte visas!). (1p)

b) Beräkna $|G|$. (1p)

c) Visa att G är en cyklisk grupp och ange explicit en generator. Bestäm sedan alla delgrupper till G. (3p)

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) Vad är stabilisatorn av $RGRGRG \in A^6$? (1p)

b) Vilka fixpunkter har r^2? (1p)

c) Använd Burnsides sats för att beräkna antalet olika halsband som kan sättas ihop av strängarna i A^6, d v s beräkna antalet banor under verkan av R.(Obs:Burnsides sats måste användas.) (3p)

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)

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? (2p)

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?

Meddelandet 0001011 tas emot, men vad var (under antagande av högst ett fel) det ursprungliga meddelandet? (3p)

6. a) Visa att polynomet $p(x) := x^2 + x + 1 \in \mathbb{Z}_2[x]$ är irreducibelt.(1p)

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

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

Visa att detta är en ekvivalensrelation. (1p)

c) Visa att det finns precis fyra ekvivalensklasser. (1p)

d) Visa att för varje polynom $0 \neq s(x) \in \mathbb{Z}_2[x]$ finns det ett polynom $t(x) \in \mathbb{Z}_2[x]$ så att $s(x)t(x) \equiv 1$. Visa att för $s(x) = x$ uppfyller $t(x) = x + 1$ att $s(x)t(x) \equiv 1$. (2p)