Lösningsskiss tenta 2026-02-27, Algebra och kombinatorik.

(1) (a) Enligt binomialsatsen är

$$\sum_{k=0}^{81} \binom{81}{k} (-5)^k 4^{81-k} = (-5+4)^{81} = (-1)^{81} = -1.$$

(b) Eftersom $6 \cdot 6 = 36 = 1$ i $\mathbb{Z}_{35}$ är $6^{-1} = 6$.

(c) Mängden $\{(1,1)\} \subset \mathbb{Z}_2^2$ är en kod som är inte linjär eftersom att $(0,0) \notin \{(1,1)\}$.

(2) (a) Vi löser uppgiften med inklusion-exklusion. Ordet SKRIDSKOSKOLA har 13 bokstäver fördelade på 3 stycken S och K, 2 stycken O och en av resterande bokstäver. Det totala antalet ord som bokstäverna i SKRIDSKOSKOLA kan skapa är därför

$$\binom{13}{3,3,2,1,1,1,1,1}.$$

Antalet av dessa som innehåller ordet SKRIDSKO kan fås genom att se SKRIDSKO som en symbol med de resterande symbolerna SKOLA. Alla dessa 6 symboler är olika, vilket ger 6! ord. De ord som innehåller SKOLA har på liknande sätt kvar symbolerna i SKRIDSKO, där det nu finns två S och två K, så totalt kan

$$\binom{9}{2,2,1,1,1,1,1}$$

ord skapas som innehåller SKOLA. När vi nu behöver räkna på hur många sätt orden SKRIDSKO och SKOLA kan uppkomma samtidigt måste vi skilja på två fall. Antingen kan båda symbolerna SKRIDSKO och SKOLA uppkomma separat, och eftersom det inte finns några andra bokstäver kvar sedan kan detta ske på 2 sätt. Det skulle också kunna vara så att symbolen SKRIDSKOLA uppkommer, vilket lämnar kvar bokstäverna SKO. Dessa fyra symboler kan då omkastas på 4! sätt. Enligt principen om inklusion-exklusion är antalet ord som inte innehåller SKRIDSKO eller SKOLA därför

$$\binom{13}{3,3,2,1,1,1,1,1} - 6! - \binom{9}{2,2,1,1,1,1,1} + 2 + 4!.$$

(b) Eftersom $133 = 7 \cdot 19$ har vi att $\phi(n) = \phi(133) = 6 \cdot 18 = 3^3 \cdot 2^2$. För att talet e ska få vara en del av en RSA-kod måste $\text{sgd}(e, \phi(n)) = 1$. Från vår primtalsuppdelning söker vi därför efter alla e i intervallet $50 \leq e \leq 60$ som ej är delbara med 2 eller 3. Dessa är $53, 55$ och 59. Alltså finns det 3 heltal e som är möjliga.

(3) (a) Vi har att $f(1) = 6 = 0$ i $\mathbb{Z}_3$, så enligt faktorsatsen kan vi faktorisera $f(x) = (x-1)g(x)$ för något polynom $g(x)$. Polynomdivision ger att $g(x) = x^4 + x^3 + x - 1$. Vi noterar att $g(0) \neq 0$, $g(1) \neq 0$ och $g(2) \neq 0$, så g har inga linjära faktorer. För att bestämma om g är irrecucibel

behöver vi undersöka om g kan skrivas som en produkt av två grad 2 polynom. Alltså, vi undrar om det går att hitta $a, b, c, d \in \mathbb{Z}_3$ så att

$$\begin{aligned} x^4 + x^3 + x - 1 &= (x^2 + ax + b)(x^2 + cx + d) \\ &= x^4 + (a + c)x^3 + (b + d + ac)x^2 + (ad + bc)x + bd. \end{aligned}$$

Vi börjar att jämföra koefficienter, dessa måste vara lika i vänsterledet och högerledet av ekvationen ovan. För konstanttermen har vi att $bd = -1$, vilket ger att en av b och d är 1 och den andra är -1. Säg att $b = 1$ och $d = -1$. Insättning av detta i koefficienten framför x ger att $c - a = 1$. Men jämförelse av koefficienten framför x^3 ger att $c + a = 1$, så dessa två ekvationer tillsammans ger att $c = 1$ och $a = 0$. Slutligen, eftersom att $b + d + ac = 1 - 1 + 0 \cdot 1 = 0$ är korrekt koefficient framför x^2 har vi att $g(x)$ kan faktoriseras som

$$g(x) = (x^2 + 1)(x^2 + x - 1).$$

Då $g(x)$ inte har några nollställen har ej heller någon av dessa fatorer något nollställe och är därför irreducibla. Faktoriseringen av $f(x)$ i irreducibla faktorer är därför

$$f(x) = (x - 1)(x^2 + 1)(x^2 + x - 1).$$

(b) Enligt handskakningslemmat är summan av graderna för alla hörn ett jämt tal. Eftersom $9 \cdot 3 = 27$ är udda finns det därför ingen graf med 9 hörn där alla har grad 3. Om en graf inte har några cykler så är det ett träd (eller en skog) och kan därför färgläggas med högst två färger. Så det kan aldrig ha kromatiskt tal 3.

(4) (a) För att visa att den ändliga mändgen A_n är en delgrupp av S_n räcker det enligt sats att visa att A_n är icke-tom och att om $\alpha, \beta \in A_n$, då är $\alpha \cdot \beta \in A_n$. Identitetspermutationen id är jämn så $\mathrm{id} \in A_n$ och A_n är icke-tom. Vi vet också att en jämn gånger en jämn permutation är jämn, så om $\alpha, \beta \in A_n$, då är $\alpha \cdot \beta \in A_n$. Mängden B_n är inte en delgrupp eftersom att identiteten id inte är en udda permutation och därför inte ligger i B_n.

(b) Att multiplicera en permutation α med transpositionen $(1\ 2)$ ger att om α kan skrivas som en produkt av k transpositioner, då kan $(1\ 2) \cdot \alpha$ skrivas som en produkt av $k + 1$ transpositioner. Så om α är jämn, då är $(1\ 2) \cdot \alpha$ udda, och om α är udda, då är $(1\ 2) \cdot \alpha$ jämn. Med andra ord, $f(\sigma) = (1\ 2) \cdot \sigma$ skickar A_n till B_n men också B_n till A_n. Så om vi definerar $g : B_n \to A_n$ med samma regel att $g(\tau) = (1\ 2) \cdot \tau$, då följer det från $(1\ 2) \cdot (1\ 2) = \mathrm{id}$ att

$$g(f(\sigma)) = g((1\ 2) \cdot \sigma) = (1\ 2) \cdot (1\ 2) \cdot \sigma = \sigma$$

och

$$f(g(\tau)) = f((1\ 2) \cdot \tau) = (1\ 2) \cdot (1\ 2) \cdot \tau = \tau,$$

så f är inverterbar med invers g. Från sats vet vi därför att f är en bijektion. Eftersom $f : A_n \to B_n$ är en bijektion vet vi att A_n och

B_n är lika stora. Dessutom vet vi att alla permutationer är udda eller jämna och att ingen permutation är båda udda och jämn, så

$$n! = |S_n| = |A_n \cup B_n| = |A_n| + |B_n| = |A_n| + |A_n|.$$

Därför är kardinaliteten av A_n givet av $|A_n| = \frac{n!}{2}$.

(c) Från (b) vet vi att $|A_4| = \frac{4!}{2} = 12$. Så enligt Lagranges sats måste storleken på K dela 12. Låt oss hitta några element i K. Vi har att $(1\ 2)(3\ 4), (1\ 2\ 3) \in K$ och $\mathrm{id} \in K$ eftersom det är en grupp. Slutenhet ger nu att

$$\begin{aligned}(1\ 2\ 3)(1\ 2\ 3) &= (1\ 3\ 2)\\ (1\ 2)(3\ 4)(1\ 2\ 3) &= (2\ 4\ 3)\\ (1\ 2)(3\ 4)(1\ 3\ 2) &= (1\ 4\ 3)\\ (2\ 4\ 3)(2\ 4\ 3) &= (2\ 3\ 4)\end{aligned}$$

alla är element i K. Detta ger att $|K| \geq 7$, så om $|K|$ ska dela 12 måste ordningen på K vara $|K| = 12$.

(5) (a) Vi behöver visa fyra egenskaper hos $(G^{op}, \star)$. Att den är sluten under $\star$, är associativ, har en identitet och har inverser.
Sluten: Tag $a, b \in G^{op}$, då är

$$a \star b = b \cdot a \in G = G^{op}$$

eftersom att $(G, \cdot)$ är sluten.
Associativ: Tag $a, b, c \in G^{op}$, då är

$$a \star (b \star c) = a \star (c \cdot b) = (c \cdot b) \cdot a = c \cdot (b \cdot a) = (b \cdot a) \star c = (a \star b) \star c$$

eftersom att $(G, \cdot)$ är associativ.
Identitet: Låt $e \in G = G^{op}$ vara identiteten i $(G, \cdot)$. Då gäller det att $e \star a = a \cdot e = a$ och $a \star e = e \cdot a = a$ för alla $a \in G^{op}$, så e är en identitet i $(G^{op}, \star)$.
Inverser: Låt $a \in G^{op}$ och låt b vara inversen till a i $(G, \cdot)$. Då har vi att $a \star b = b \cdot a = e$ och $b \star a = a \cdot b = e$, så $b = a^{-1}$ i $(G^{op}, \star)$ och $(G^{op}, \star)$ är en grupp.

(b) För att $f : (G, \cdot) \to (G^{op}, \star)$ ska vara en isomorfism måste $f(a \cdot b) = f(a) \star f(b)$ för alla $a, b \in G$. Eftersom att $(G, \cdot)$ inte är en kommutativ grupp kan vi ta $x, y \in G$ så att $x \cdot y \neq y \cdot x$. Då har vi att $f(x \cdot y) = x \cdot y$, men att $f(x) \star f(y) = x \star y = y \cdot x$, så $f(x \cdot y) \neq f(x) \star f(y)$.
För $g : (G, \cdot) \to (G^{op}, \star)$ har vi att

$$g(a \cdot b) = (a \cdot b)^{-1} = b^{-1} \cdot a^{-1} = a^{-1} \star b^{-1} = g(a) \star g(b)$$

för alla $a, b \in G$. Eftersom inverser är unika är g injektiv och eftersom alla $a \in G$ kan skrivas som $a = (a^{-1})^{-1}$ har vi att g är surjektiv. Alltså är g bijektiv och uppfyller att $g(a \cdot b) = g(a) \star g(b)$, så g är en isomorfism.

(6) Låt G vara gruppen av symmetrier av en kvadrat. Om X är mängden av alla utplaceringar av damer och kungar på rutnätet, då vill vi veta hur många banor som G har på X. Dessa banor räknar vi med hjälp av Burnsides lemma.

När $g = \text{id}$ är identitetselementet ges dess fixpunktmängd av hela X. Så

$$|F(g)| = |X| = \binom{16}{12, 2, 2}$$

eftersom det finns 16 rutor totalt och den inbördes positionen på de 12 blanka rutorna, de två damerna och de två kungarna spelar ingen roll.

För $g = r$, en rotation med ett fjärdedels varv, gäller att $|F(g)| = 0$. Detta eftersom att om vi fokuserar på kungarna, då kommer rotationen förflytta en kung från en av de fyra kvadranterna av rutnätet till en intilliggande kvadrant. Därmed kommer upprepade rotationer göra så att kungarna måste passera all fyra kvadranter av rutnätet. Men vid en fixpunkt skulle de två kungarna bara kunna besöka två kvadranter, de som kungarna redan står på. Alltså kan inga fixpunkter finnas. Samma resonemang ger att $|F(r^3)| = 0$.

För $g = r^2$, en rotation med ett halvt varv, så finns det fixpunkter. En sådan rotation tar en kung eller en drottning från övre halvan av rutnätet till undre halvan och vise versa. Så om vi bestämmer var kungen och drottningen på den övre halvan är placerade, då bestämmer det en unik utplacering som är en fixpunkt. Så $|F(g)| = 8 \cdot 7 = 56$ där vi har 8 möjliga val för drottningen på övre halvan och sedan 7 rutor kvar att placera en kung på. För $g = s_h$, speglingen i den horisontella linjen som delar den övre halvan av rutnätet från den undre halvan är argumentet precis detsamma som för rotation med ett halvt varv, så $|F(g)| = 56$. På samma sätt är $|F(s_v)| = 56$ där s_v är spegling i den vertikala linje som delar rutnätet i en höger och en väster sida.

Slutligen, för $g = s_d$, en spegling i en linje som går genom en av de två diagonalerna, då har vi också en icke-tom fixpunktmängd. Om vi har en utplacering utan kungar eller damer på diagonalen vi speglar igenom, då finns det 6 rutor under diagonalen och utplacering av en kung och en dam där bestämmer unikt var en kung och en dam måste vara över diagonalen för att få en fixpunkt. Detta ger alltså $6 \cdot 5 = 30$ fixpunkter. Om det bara finns damer på diagonalen, då måste båda damerna var på diagonalen, och utplaceringen av dessa kan göras på $\binom{4}{2} = 6$ sätt. Som innan bestämmer sedan en kung under diagonalen unikt en kung över diagonalen för att få en fixpunkt, vilket ger $6 \cdot 6 = 36$ fixpunkter till. Av symmetrin finns det sedan 36 fixpunkter till när det bara är kungar på diagonalen. Till sist kan det även hända att både kungarna och damerna är på diagonalen, vilket kan se på $\binom{4}{2,2} = 6$ sätt. Detta ger att $|F(g)| = 30 + 36 + 36 + 6 = 108$. Eftersom det inte är någon skillnad på det två diagonalerna gäller öven att $|F(g)| = 108$ för speling i den andra diagonalen.

Enligt Burnsides lemma är antalet utplaceringar därmed

$$\frac{1}{|G|} \sum_{g \in G} |F(g)| = \frac{1}{8} \left(\binom{16}{12, 2, 2} + 56 \cdot 3 + 108 \cdot 2 \right) = 1403.$$