VG-listan.

GRUPPER

G 2)

a) En tankspridd undervisare i Abstrakt Algebra skulle ge exempel på en delgrupp av $U(91)$. Han listade klasserna av $1, 9, 16, 22, 53, 74, 79, 81$, vilket är orimligt, varför? Hitta den felande klassen.

b) Ange två klasser g, h sådana att alla element i delgruppen kan skrivas på formen $g^i h^j$, $0 \le i, j \le 2$.

c) Använd detta till att verifiera att den verkligen är en grupp. (3 p)

G 3) Låt A och B vara två grupper och $a \neq 1$ resp. $b \neq 1$ element i dessa. Anta att deras ordningar $o(a)$ och $o(b)$ är relativt prima. Bilda deras direkta produkt $A \times B$. Låt H vara en delgrupp av denna produkt. Anta att $(a, b) \in H$. Visa att $(a, 1)$ och $(1, b)$ tillhör H. Ledning: betrakta $(a, b)^{o(a)}$, $(a, b)^{o(b)}$.
(3 p)

G 4) Anta att den icke-abelska gruppen G har sex element.

a) Anta att alla element utom e har ordning två; visa då att det finns två element a, b med $ab = ba$ vilket skulle ge en delgrupp av ordning 4.

b) Visa nu att den innehåller två element av ordning tre och tre av ordning två.

c) Låt g ha ordning tre och h ha ordning två. Visa att $hgh^{-1} = g^2$ och att detta visar att $G \simeq D_3$ (eller, ekvivalent, S_3)

(4 för hela)

G 6) Betrakta verkan av S_6 på polynomen $f(x_1, \ldots, x_6) = (x_1 - x_4)(x_2 - x_5)(x_3 - x_6)$ samt $g = f^2$, enligt $f^\sigma(\ldots, x_j, \ldots) = f(\ldots, x_{\sigma(j)} \ldots)$

Låt H_f och H_g beteckna stabilisatorgrupperna.

a) Till varje permutation i dessa båda grupper kan naturligt ordnas en permutation i S_3; denna tillordning ska vara en surjektiv homomorfism. Beskriv! Bestäm i vardera fallet kärnan och härur ordningarna av H_f, H_g.

b) Visa att H_g innehåller diedergruppen D_6, representerad som permutationsgrupp på hörnen. Hur är det med H_f?

c) Ange därpå, med korta motiveringar, antalet fixerande permutationer i H_g av varje tänkbar cykelstruktur

(2+2+2 p)

G 7) (tre delar)

a) Här är ett 15-spel i utgångsläget:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 15 & 14 & \end{pmatrix}$$

Ett tillåtet drag flyttar in en bricka i tomrummet, vertikalt eller horisontellt, så att tomrummet kan hamna i vilken som helst av de 16 positionerna.

Efter varje drag kan vi avläsa en permutation av talen $1, 2, \ldots, 15$ - vi tar då raderna uppifrån och avläser varochen från vänster till höger.

I diagrammet ovan är denna permutation transpositionen $(14 \quad 15)$

Beskriv hur tomrummets position bestämmer permutationens tecken.

b) Visa att följande inte kan uppnås:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & \end{pmatrix}$$

c) Bonus: Kan du ange en följd av drag, från läget i a), som ställer alla 15 talen i rätt ordning, men med tomrummet någon annanstans? (jag vet just nu inte svaret!)

(1+2+? p)

G 10)

a) Betrakta gruppen G av invertibla 2/2-matriser över kroppen $\mathbf{Z}/(7)$, alltså matriser med determinant $\neq 0$. Bestäm antalet element (första kolonnen ska vara skild från nollkolonnen, den andra ska inte vara en multipel av den).

b) Betrakta matrisen

$$g = \begin{pmatrix} m & 0 \\ 0 & n \end{pmatrix}$$

där m och n är skilda element i $\mathbf{Z}/(7)$ båda $\neq 0$. Bestäm $C(g)$ (direkt ansats och räkning) och härur antalet element i $cl(g)$.

c) Visa att alla konjugat

$$xgx^{-1} = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$$

har egenskaperna $ps - qr = mn, p + s = m + n$ (här hjälper det med rejäla kunskaper i lineär algebra). Bestäm antalet sådana matriser och visa att de precis motsvarar $cl(g)$. Tips: särbehandla fallen $p, s = m, n$ och $p, s \neq n, m$.

d) Generalisera a), b), c) till godtyckligt primtal p

RINGAR

R 1) α är ett invertibelt element i en kommutativ ring R med etta. α har en additiv och en multiplikativ ordning, kalla dem a resp. m. Invertibla matriser med element i R bildar en grupp G. (invertibla matriser kan kännetecknas av att determinanten är invertibel, men vi behöver inte detta).

a) Vad är ordningen i G av matrisen

$$\begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix}?$$

(bryt ut α först). Svaret ska uttryckas m h a heltalen m, a.

Verifiera ditt svar i fallet att α är klassen av 2 eller 3 i $\mathbf{Z}_7$

b) Bestäm ett slutet (ändligt) uttryck för matrisen g^n, där

$$g = \begin{pmatrix} 1 & \lambda & 0 \\ 0 & 1 & \lambda \\ 0 & 0 & 1 \end{pmatrix}$$

(räkna ut några låga potenser, gissa, och inducera!)

Bestäm sedan ordningen av

$$\begin{pmatrix} \alpha & 1 & 0 \\ 0 & \alpha & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

där α är en nollskild klass modulo primtalet p.

(2+2 p)

R 2) Ett *kvadratfritt tal* är ett positivt heltal som inte är delbart med något tal av formen m^2, där m är ett heltal ≥ 2. Låt d vara ett kvadratfritt positivt heltal $\equiv 1 \pmod 4$. Visa att talen av formen

$$m + n\frac{\sqrt{d}+1}{2}; \quad m, n \in \mathbf{Z}$$

utgör en ring och att de satisifierar andragradsekvationer (eller lineära ekvationer, om $n = 0$, förstås) med heltalskoefficienter och högstagradskoefficienten 1. (3 p)

R 5)

a) Verifiera att avbildningen $\varphi : \mathbf{Z}[i] \to \mathbf{Z}/(13)$ given av $\varphi(a + ib) = \overline{a} + \overline{5b}$ är en ringhomomorfism
b) Beskriv, och åskådliggör geometriskt kärnan för φ. Den är som bekant ett principalideal. Bestäm en generator, ur den geometriska bilden (du behöver studera *beviset* för att $\mathbf{Z}[i]$ är ett P.I.D.), och/eller på annat sätt.
c) Ange surjektiva homomorfismer från $\mathbf{Z}[i]$ till $\mathbf{Z}/(11)$ och $\mathbf{Z}/(17)$ eller visa att det inte går. (1+1+1 p)

R 6) Vi betraktar ringen $R = \mathbf{Z}[\sqrt{3}]$ bestående av alla talen $m + n\sqrt{3}$ där m, n är heltal (verifiera ringegenskapen). Vi vill beskriva restringen modulo idealet $(\sqrt{3})$.

a) Visa att $\varphi : \mathbf{Z} \to R$ som avbildar m på dess klass modulo $(\sqrt{3})$ är en surjektiv ringhomomorfism.
b) Visa att dess kärna innehåller idealet (3).
c) Slut att att R/I är isomorf med $\mathbf{Z}_3$.
d) Bestäm på samma sätt restklassringen av R modulo $1 + \sqrt{3}$.

(4 p för hela)

R 7) Visa att ekvationen $x^2 + y^2 - 3t^2 - 3u^2 = 0$ saknar heltalslösningar. Ledning: faktorisering i $\mathbf{Z}[i]$. (3 p)

R 12) Utöver vanliga ideal i ett P.I.D. R kan man betrakta *brutna* ideal, som ligger i ringens bråkkropp (field of fractions), och är av typen

$$\frac{p}{q}R, \qquad p, q \in R$$

och som alltså består av alla element av typen

$$\frac{rp}{q}, \qquad r \in R$$

Beskriv summa och snitt av idealen

$$\frac{1}{p}R \text{ samt } \frac{1}{q}R$$

i delbarhetstermer (liknande dem för hela ideal). Sen kan du vilja göra samma för summa och snitt av två godtyckliga brutna ideal. (3 p)

R 14) De flesta böcker visar att ändliga integritetsområden är kroppar.

a) Visa tillspetsningen: i en ändlig ring (kommutativ med etta) gäller att alla icke-nolldelare är invertibla. Härma bokens bevis så långt du kan.
b) En liknande sats är denna: anta att ringen R (kommutativ med etta) innehåller en kropp k och är ett ändligdimensionellt vektorrum över k (exempel: $k[X]/(m(X), m(X) \neq 0)$). Visa att varje icke-nolldelare är invertibel. Ledning: ett lämpligt antal potenser av elementet ifråga är lineärt beroende. (2+2 p)

R 16) (fyra delar)

a) Låt $\omega = (1/2)(1+\sqrt{5})$ Bilda $R = \mathbf{Z}[\omega]$ bestående av elementen $z = m + n\omega$ där m, n är heltal. Verifiera att detta är en ring.

b) Sätt $N(m+n\omega) = m^2 + mn - n^2$. Visa att $N(rs) = N(r)N(s)$

c) Begagna denna till att visa att R är en euklidisk ring, därmed även PID, ungefär som för de gaussiska heltalen.

d) Bestäm element r, s, med $r \neq 1, N(r) = 1; N(s) = -1$. Visa med dessas hjälp att ringen har oändligt många invertibla element. (1+1+1+1 p)

KROPPAR

Kommentar till beteckningar. Låt k vara en kropp, och θ ett element i kroppen $K \supset k$. $k[\theta]$ betecknar den minsta *ring* som innehåller θ och kroppen k. $k(\theta)$ är den minsta *kropp* som innehåller k och θ. Dessa båda är lika om och endast om θ är algebraisk över k, dvs. rot till en polynomekvation med koefficienter i k.

Om datorstöd. En del uppgifter kräver räkning, t ex polynomdivision mod p. Man bör inte göra långa kalkyler för hand. Med så små gradtal som är aktuella klarar man sig bra med **matlab**:s kommandon *conv* och *deconv* för multiplikation och division med rest, vidare *mod* för att reducera allting modulo p. Kursarean har en m-fil som utför Euklides modulo p.

När det uttryckligen står handräkning är det det som gäller. Självklart förbjuder jag ingen att kontrollera framräknade svar, faktoriseringar, etc. i **maple** (det torde spara tid åt mig, om inte annat), men räkningarna ska presenteras på ett sådant sätt att den teoretiska förståelsen aldrig kan betvivlas, dvs. det ska synas *vad du gjort*.

K 1) Visa, genom att beskriva den, att spaltningskroppen av $x^9 + 1 \in \mathbf{Z}_2[X]$ har grad 6 över $\mathbf{Z}_2$. (3 p)

K 3) Betrakta polynomet $p(X) = X^5 - 1$ i $\mathbf{Q[X]}$

a) Beskriv en kroppsutvidgning $\mathbf{Q}(\theta)$ där p får en rot θ, ange speciellt dess grad.

b) Hur många rötter har $X^5 - 1 = 0$ i denna kropp?

c) Ange minimalpolynomet $m(X)$(över $\mathbf{Q}$) för

$$\theta + \frac{1}{\theta}.$$

Lös ekvationen $m(X) = 0$ och härled härur ett uttryck för $\cos(2\pi/5)$, med ett enda rotmärke. Vad är sinus för samma vinkel? (1+1+1 p)

K 4)

a) Visa att ringen $\mathbf{Q}[\sqrt{2}+\sqrt{3}]$ är en kropp. Bestäm också (kanske först) minimalpolynomet för $\theta = \sqrt{2}+\sqrt{3}$ över $\mathbf{Q}$

b) Visa därpå att $\mathbf{Q}[\sqrt{2}, \sqrt{3}]$ är en kropp och att de båda kropparna är lika.

c) Bestäm tillsist $1/\theta$, uttryckt som tredjegradspolynom i θ, med rationella koefficienter. (1+1+1)

K 8)

Betrakta polynomet $X^p - X - 1$ över kroppen $\mathbf{Z}_p$, p primtal. Låt α vara en rot i en utvidgningskropp. Beskriv enkelt de olika rötter som erhålles genom upprepad användning av Frobenius. Hur många är de? Är polynomet irreducibelt? (3 p)

K 9) K är en kropp med 27 element. β tillhör inte primkroppen. Vilka är dess möjliga ordningar i den multiplikativa gruppen av K? Visa att antingen β eller $2 \cdot \beta$, men inte bägge, har maximal ordning, dvs. genererar multiplikativa gruppen. (3 p)

K 12)

a) $k = \mathbf{Z}/(2)$. Betrakta polynomet $X^{11} + 1 \in k[X]$. Det har roten $\theta \neq 1$ i en utvidgningskropp med 2^d element. Visa att $d \geq 10$ (titta på ordningar i multiplikativa gruppen) och slut av detta att polynomet $(X^{11} + 1)/(X + 1) \in k[X]$ är irreducibelt. (3 p)

b) (forts.) Gör motsvarande undersökning för $X^{13} + 1 \in k[X]$ och $X^{17} + 1 \in k[X]$ (a+2)

c) (forts.) Beskriv faktoriseringen av $X^{21} + 1 \in k[X]$ genom att ange de irreducibla faktorernas grad, samt antalet av varje grad. (3 p)

K 15) $m(X)$ är ett irreducibelt (moniskt) polynom i $k[X]$ där $k = \mathbf{Z}_p$, p primtal. Bilda nu kvotringen $k[X]/(m(X)^2)$. Visa att ordningen av varje invertibel klass är en faktor i $p \cdot (p^d - 1)$ och att detta visar att gruppen av invertibla klasser i denna ring inte är cyklisk.

(3 p)

K 18) p är ett udda primtal. Vi ska avgöra om (klassen av) 2 är en kvadrat i $k = \mathbf{Z}_p$ i fallen $p \equiv 1, 3, 5, 7$ (mod 8).

Låt θ var ett element med $\theta^4 = -1$ i någon utvidgningskropp av $k = \mathbf{Z}_p$. Bilda $s = \theta - \theta^3$ och visa att $s^2 = 2$.

Avgör m h a Frobenius i vilka av ovanstående fyra fall som s tillhör $k = \mathbf{Z}_p$ och dra slutsatser! (3 p)

K 19) En primitiv n:e rot till $1 \in K$, K kropp, är ett element $\alpha \in L$, L utvidgning av K, sådan att $\alpha^n = 1$, men $\alpha^m \neq 1$ för varje naturligt tal $m < n$.

a) Ange alla primitiva 12:e enhetsrötter i kroppen $\mathbf{C}$. Verifiera att de uppfyller en irreducibel ekvation med koefficienter i $\mathbf{Z}$. Ange den!

b) Verifiera att varje udda primtal $p > 3$ uppfyller $p^2 \equiv 1 \bmod 12$. Slut av detta att ditt funna polynom, $q(X)$, är reducibelt modulo varje udda primtal p.

c) Bestäm något p sådant att det sönderfaller i förstagradsfaktorer modulo p. (4 p för hela)

K 20) $k = \mathbf{Z}_3$. K är en utvidgning av grad 4, med 81 element. Söker element av (gruppteoretisk) ordning 80. Först tar vi en rot α till endera av de de irreducibla faktorerna till $X^8 + 1$ - bestäm dessa. Vilken ordning har denna rot? Bilda sedan $\alpha + \alpha^2$ och bestäm *dess* ordning. Hur hittar du nu ett element av ordning 80? Bestäm dess minimalpolynom samt dess övriga rötter, som polynom (grad högst 3) i α.

KINESSATSEN, LINEÄR REKURSION

C 1) Vi fortsätter uppgift G2. Betrakta ringen $\mathbf{Z}_{91}$; ge dess CRT-uppdelning som direkt summa (produkt) av kroppar. Bestäm idempotenterna Beskriv enhetsgruppen $U(91)$ som direkt produkt av enklare grupper. Du behöver karakterisera de invertibla elementen i en produktgrupp. Använd detta till att visa att gruppen inte är cyklisk. Bestäm också möjliga ordningar av olika element. Ange nu elementen av ordning 3 (eller 1) i produktgruppen. Använd dessa, och idempotenterna, till att bestämma motsvarande element i $U(91)$. Jämför sedan svaret med uppgift G2 (3).

C 2)

a)

$m(X)$ är ett irreducibelt polynom i $k[X]$, $k = \mathbf{Z}_p$.. Som bekant har kroppen $K = k[X]/(m(X))$ $p^d - 1$ invertibla element, där d är graden av $m(X)$.

a) Hur många invertibla element, resp. nolldelare är det i ringen $k[X]/(m(X)^e$, $e \geq 1$?

b) $m_1(X), m_2(X) \in k[X]$ är relativt prima (men kanske reducibla).

Anta att antalet invertibla element i ringarna $k[X]/(m_i(X))$ är r_i, $i = 1, 2$. Vad är antalet invertibla element i ringen $k[X]/(m_1(X) \cdot m_2(X))$?

c) $p(X) \in k[X]$ givet, grad $=d$, ej delbart med X. Anta att klassen av X i $k[X]/(p(X))$ (nu garanterat invertibel) har multiplikativa ordningen $p^d - 1$. Visa (detta är huvuduppgiften, använd de föregående) att $p(X)$ är irreducibelt (för att visa att polynom är primitivt behöver man alltså bara bevisa ena hälften av villkoret) (2+1+2 p)

C 3)

a) Visa att heltalskongruensen

$$ax + b \equiv 0 \pmod{m}$$

är lösbar om, och endast om, (a, m) är en faktor i b. Ange antalet lösningar, modulo m. Tips: anknyt till beviset för C.R.T.

b) Studera sista exemplet i avsnitt II av modulstencilen, Chapter 17. Vad är i allmänhet bild och kärna av (grupp)homomorfismen

$$\psi : \mathbf{Z}/(m) \oplus \mathbf{Z}/(n) \to \mathbf{Z}/(mn)$$

given av

$$\psi(p + (m), q + (n)) = (pn + qm + (mn)$$

om vi inte förutsätter $(m, n) = 1$?

Båda genereras (som grupper) av et enda element och kan beskrivas som kvotgrupper av $\mathbf{Z}$. Konstruera nämligen lämpliga homorfismer från $\mathbf{Z}$ till Kerψ och Imψ och bestäm kärnan av *dessa* homomorfismer.