Examinationsuppgifter, G och 3

Lösningar lämnas i det röda tråget, c:a 3 meter NV till NNV om mitt rum. **INTE** i mitt postfack!

Lösningarna ska vara välskrivna och läsliga, på ena sidan av varje ark. Jag tar inte emot lösningar per epost. Dra in formeltext hellre för ofta än för sällan. Luft! Jag behöver plats för rättningskommentarer.

Försättsblad: Namn, program, epost, personnummer. Ange vilka uppgifter du löst.

Allt samarbete kring examinationsuppgifterna, med andra kursdeltagare eller utomstående, är förbjudet. Spar tid och tjäna poäng genom att *kontrollera* svaren, pröva "låga" fall, osv. Felaktiga lösningar och svar leder i allmänhet *inte* till retur. Lämna alltså med marginal.

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 hel del m-filer, samt en och annan python-modul som gör lite tråkiga saker.

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*.

Grupper, Lagrange, gruppelements ordning

W 1)Bestäm heltalslösningar, helst alla, till $m \cdot 38 + n \cdot 100 = 1, 2, 4$ i de fall det går. Motbevis annars! (1 p)

W 2) Finn inverser (eller motbevisa existens) till klassen av 3 modulo 7, 5 modulo 6, samt 18 och 33 modulo 100. (1 p)

W 3) (fyra delar)

a) Beskriv alla de möjliga cykelstrukturerna för permutationer av ordning 2,3, 6, 12, 30 i S_{12}
b) g, h är element i gruppen G. Visa att produkterna gh och hg har samma ordning
c) H är en delgrupp av gruppen G. Anta att $g \in G$ kommmuterar med alla element i gruppen H. Visa, att samma gäller om g^{-1}

d) Gruppen G är cyklisk av ordning 3672. Jag vill avgöra om elementet $g \neq e$ genererar G. Fyra potenser av g behöver bestämmas. Vilka? Motivera?

(2+2+1 +1 p)

W 4)

a) Visa att klasserna av 4,8,12,16 i $\mathbf{Z}_{20}$ bildar en *multiplikativ* grupp. Ange speciellt dess identiska element. Är den cyklisk?

b) Samma uppgift för $7, 35, 49, 77$ i $\mathbf{Z}_{84}$

c) Ange de klasser i den additiva gruppen $\mathbf{Z}_{40}$ som har ordning exakt $= 10$.

(2+1+1 p)

W 5)

a) Gruppelementet a har ordning 15. Vilka är ordningarna av a^3, a^4, a^5, a^6, a^8?

b) Gruppen G har 8 element av ordning 10 Ange antalet cykliska delgrupper av ordning 10.

c) Bestäm alla cykliska delgrupper av $U(30)$ Börja med att bestämma gruppens ordning.

(1+2+1 p)

W 6)

Vi betraktar en regelbunden 6-hörning. Diedergruppen D_6 består av sex vridningar (inklusive identiteten) och sex speglingar. Hörnen numreras moturs. r är vridning 60 grader moturs. s är spegling i den diagonal som förbinder hörnen 1,4. Beskriv r och s som permutationer, på disjunkt cykelform (obs. i fortsättningen att numren 1-6 alltid står för fixa lägen och således inte "följer med" hörnen vid vridning eller spegling)

a) Bestäm på cykelform, och beskriv geometriskt, produkterna

rs, sr, rsr^{-1}, srs

b) Beskriv nu samtliga 6 speglingar som uttryck i r och s

c) I en godtycklig diedergrupp D_n låter vi r och s vara en vridning respektive en spegling. Låt g vara ett godtyckligt element. Beskriv på enklast möjliga sätt symmetrierna grg^{-1} och gsg^{-1} (svaret kan bero på g).

d) Om s, t är två speglingar, finns då säkert ett g sådant att $s = gtg^{-1}$?

(2+2+2+2 p)

W 7) Betrakta diedergruppen D_6 bestående av de 12 symmetrierna av en regelbunden 6-hörning. Bestäm, med vederbörliga verifikationer, två delgrupper av ordning 6, en abelsk och en icke-abelsk. (3 p)

W 8) Delgruppen A_5 av S_5, den *alternerande* gruppen beskrivs i böckerna. Ange cykelstrukturerna för dess element och (det är huvuduppgiften) visa att varje element är en produkt av 3-cykler $(m\,n\,p)$

Det räcker förstås att göra det för ett element av varje möjlig cykelstruktur.

(3 p)

W 9) Vi tittar på n/n–matriser med element i kroppen $\mathbf{Z}_p$, p primtal. Precis som för reella matriser gäller invertibilitet om och endast om determinanten $\neq 0$. (I godtycklig kommutativ ring med etta är kravet att determinanten är invertibel).

Invertibla matriser av fixt format visas lätt bilda en grupp.

Vi låter nu p=2.

a) (Uppvärmning) Bestäm en invertibel 2/2-matris av ordning 2 och en av ordning 3.

b) Bestäm ordningen av matriserna

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

c) Visa att matriserna

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

bildar en delgrupp, och bestäm dennas ordning.

d) Vilken slutsats kan dras enbart ur b) och c) om minsta tänkbara ordningen av gruppen av invertibla 3/3-matriser? (i själva verket är detta den sanna ordningen).

(4 poäng för hela uppgiften)

W 10) Räcker angivelserna $o(a) = 4; o(b) = 2, a^3 b = ba$ för att bestämma ordningen av ab? Isåfall, gör det. (2 p)

W 11) I en grupp gäller

a) $a^4 = e, ab = ba^2$. Visa:$a = e$

b) $a^6 = e, ab = ba^3$. Visa:$a^2 = e, ab = ba$.

c) $a^6 = e, ab = ba^2$. Visa: $a^3 = e, aba = b$ (1+1+1 p)

W 12) G är en grupp, H en delgrupp. $g \in G$ är ett element sådant att $g^n \in H$. Låt m vara det minsta positiva heltal för vilket $g^m \in H$. Visa att $m|n$. (Härma teorin för gruppelements ordning). (3 p)

W 13)

a) Låt n vara udda. Visa att avbildningen $U(2n) \to U(n)$ given av $m + (2n) \to m + (n)$ är en homomorfism och bijektiv. Beskriv också den inversa isomorfin. I det senare fallet bör du börja med att granska lite exempel.

b) Är $U(10)$ och $U(20)$ isomorfa? (2+1 p)

W 14)

a) Visa att permutationerna $(1\,2\,4), (1\,3\,4)$ kan uttryckas som produkter innehållande faktorerna $(1\,2\,3), (2\,3\,4)$ enbart.

b) Vi är nu i S_n. Visa att den cykliska permutationen $(1\,x\,n)$ kan uttryckas som produkt av 3-cykler där antingen 1 eller n saknas. Deluppgift a) är specialfallet $n = 4$

c) Visa, t ex medels induktion över n, att varje 3-cykel i S_n, $n \geq 3$ är produkt av "enkla" 3-cykler av formen $(m \quad m+1 \quad m+2)$. Exemplifiera för $(1\,3\,5) \in S_5$

(4 p för hela uppgiften)

W 15)

Anta känt (lätt men stökigt att skriva upp) att S_n genereras av alla transpositioner (i, j). Visa att S_n genereras av alla $(1, j)$; eller av alla $(j, j + 1)$; eller av $(1, 2, \ldots, n)$ och $(1, 2)$. (3 p)

W 16) G är en ändlig abelsk grupp. Låt g vara ett element av maximal ordning d. Vi vill visa att varje element h har en ordning som är en faktor i d. Anta att $\mathrm{ord}(h) \not| d$. Låt primfaktorn p ingå i $\mathrm{ord}(h)$ till högre potens än i d. Skapa med dess hjälp ett element av ordning $p \cdot ord(g)$ och härled ur detta en motsägelse. (3 p)

PID, restklassringar, Euler och Fermat, entydig faktorisering

W 17)
 a) Beräkna $5^{15} \pmod 7$ och $7^{13} \pmod{11}$. Kort lösning, för hand!
 b) $(5^{97}+11^{33})^8 \pmod{24}$, kort lösning, för hand. (1+1 p)

W 18)
 a) n naturligt tal. Visa att $n^{111}-n$ är delbart med 11.
 b) Visa att $n^5/5+n^3/3+7n/15$ är ett heltal.
 d) Visa att $n^9+2n^7+3n^3+4n$ är delbart med 5.
 e) Anta att 7 inte är en faktor i n. Visa att 7 är en faktor i $n^{12}-1$. (1+1+1+1 p)

W 19) När jag flyttade till Linköping 1970 gick Rydsbussen i 11-minuterstrafik under 11 timmar av dagen (dvs. 60 turer). Uppvärmning:
 a) Om första turen gick 7.03, när gick den 11:e turen?
 b) När gick den första turen med minuttal 17?
 Själva uppgiften:
 c) vad var det roliga med den tidtabellen?
 Om du tyckte du fick lösningen för enkelt, lös då uppgift c) även i fallet Vallabussen, som då gick i 13-minuterstrafik i 13 timmar (60 turer). Vad är det väsentliga med talen 11, 13? (2 p)

W 20) n är ett tal vars alla primfaktorer är större än 61. Visa att $n^{60}-1$ är delbart med $16\cdot 9\cdot 25\cdot 7\cdot 11\cdot 13\cdot 31\cdot 61$ (3p)

W 21)
 a) Bestäm multiplikativa inversen till $2X+3$ i ringen $\mathbf{Z}_5[X]/(X^2+X+2)$
 b) $R=\mathbf{Z}_7[X]$. Låt $I=(X^2+6X+3)$, resp. $I=(X^2+6X+1)$
 Vilken (vilka) av ringarna R/I är en kropp? Motivera, och ange inversen av klassen av $X+2$, i de fall den existerar. (1+2 p)

W 22) Dela upp följande polynom i $\mathbf{Z}_2[X]$ i irreducibla faktorer:
 a) $X^7+X^4+X^2+X+1$
 b) X^7+X^3+1
 c) X^6+X^4+1 (3 p)

W 23) p är ett primtal, n ett heltal ≥ 2. Visa att polynomet X^n+pX+p^2 är irreducibelt över $\mathbf{Z}[X]$, således över $\mathbf{Q}[X]$.
 T ex, genom att utnyttja att $\mathbf{Z}_p$ är en kropp, visa först att en eventuell faktorisering måste ha fasonen

$$(X^k+pg(X))(X^{n-k}+ph(X))$$

 (3 p)

W 24) Betrakta ringen $\mathbf{Z}_2[X]/(X^3+X^2+X+1)$. Ange antalet element. Ange för varje nollskilt element a antingen en invers eller ett nollskilt element med $ab=0$. Varför finns de senare? (3 p)

W 25) (tre delar)
 Vi betraktar ideal i ringen R, genererade av flera element.
 a) Visa att $(a,b)=(a+tb,b)$ och $(a,b)(c,d)=(ac,ad,bc,bd))$

b) Man kan visa att ringen $\mathbf{Z}[\sqrt{6}]$ bestående av talen $m + n\sqrt{6}, m, n \in \mathbf{Z}$ är ett PID. Visa ideallikheterna $(2, \sqrt{6}) = (2 + \sqrt{6}), (3, \sqrt{6}) = (3 + \sqrt{6})$ Ange också en enda generator till vartdera av idealen $(5, \sqrt{6})$ och $(4, \sqrt{6})$.

c) Ringen $\mathbf{Z}[i\sqrt{5}]$ är *inte* ett PID. T ex är idealen $(2, 1 + i\sqrt{5}), (3, 1 + i\sqrt{5})$ och $(7, 3 - i\sqrt{5})$ inte principala, vilket man kan se genom att undersöka gemensamma faktorer. Gör det.

d) (forts. av c)) Visa att produkten av det första och det tredje idealet genereras av $3 - i\sqrt{5}$; visa sedan att även produkten av de båda första idealen är ett principalideal.

(1+2+1+2 p)

W 26)

a) Dela upp 12 och $6 + 8i$ i irreducibla faktorer i ringen $\mathbf{Z}[i] = R$

b) Samma ring. Bestäm en generator q till idealet $(15, 3 + i) = J$.

c) Bestäm en multiplikativ invers till $66 + 171\, i$ i ringen R/J. (1+1+1 p)

W 27) Vilka av följande lineära diofantiska ekvationer är lösbara i $\mathbf{Z}[i]$:

a) $a(1 + 2i) + b(3 + i) = 1$

b) $a \cdot 2 + b(3 + i) = 1 - i$

c) $a(4 + i) + b(3 + 2i) = 1$

Lös där det går, bevisa olösbarhet eljes. Obs. att de sökta a, b är komplexa heltal.

(1+1+1 p).

W 28) Betrakta ringen $R = \mathbf{Z}_2[X]/(X^5 + X + 1)$. Låt α beteckna klassen av X modulo $X^5 + X + 1$. Verifiera att α är ett invertibelt element, som uppfyller $\alpha^{21} = 1$. Är 21 dess sanna ordning? Förklara varför detta visar att R inte kan vara en kropp.

Vad säger då detta i sin tur om polynomet $X^5 + X + 1$? Verifiera denna slutsats! (3 p)

W 29)

a) Betrakta talen $0, 1, \pm i, 2, 1 \pm i, 2i, 3, 1 \pm 2i$ i ringen av gaussiska heltal. Sortera dem i inbördes olika restklasser modulo $2 + i$. Bestäm först en representant för varje klass, och därmed klassernas antal.

b) Låt $R = \mathbf{Z}[i]$. Visa att ringen $R/(2 + 2i)$ inte är en kropp. Vilket är det minsta positiva heltal som ingår i idealet $(2 + 2i)$?

c) Vi fortsätter uppgift b).

Visa att det finns (minst) en representant $m + ni$, för varje klass, med $|m| \leq 1, -1 \leq n \leq 2$; bestäm härur en representant för varje klass, och därmed deras antal. Vilka av dem är invertibla?

d) Härur, eller på annat sätt, visa att varje gaussiskt heltal $m + ni$, av udda norm, är associerat till exakt ett tal som är $\equiv 1 \pmod{2 + 2i}$. Två tal är associerade om de skiljer sig åt med en invertibel faktor.

$(4 \cdot 1$ p)

W 30) Betrakta ringen $R = \mathbf{Z}_7[X]$

a) Beskriv enklare summan och snittet av idealen $(X^2 + 2)$ samt $(X^3 + 3X^2 + X + 3)$

b) Samma uppgift för idealen $(X^2 + 1)$ och $(X^3 + 3X^2 + X + 3)$

c) Betrakta restklassringen $R/(X^2 + 1)$. Beskriv ett entydigt sätt att representera varje restklass. Hur många är de?

d) Som c), men modulo $(X^4 + 1)$ Kan du ange två klasser vilkas produkt är nollklassen?

(3 p)

W 31) (tre delar)

a) R är ett PID, a är ett nollskilt och icke invertibelt element. Vi betraktar ringen $S = R/(a)$. Visa att klassen av b, är nolldelare om idealet $d = (a, b)$ är ett äkta ideal i R och invertibel om $(a, b) = R$. Något tredje gives alltså inte (härma situationen i $\mathbf{Z}$)

b) Bestäm alla invertibla element och nolldelare i ringen $R/(X^2 + 1)$ där $R = \mathbf{Z}_{13}[X]$, speciellt deras respektive antal.

c) Samma uppgift i ringarna $R/(X^2 + 1)^2$ där $R = \mathbf{Z}_{13}[X]$ och $\mathbf{Z}_7[X]$. Och, tillsist, med exponenten $e > 1$ istf. 2. (1 + 2 p)

W 32) Irreducibilitet: Läs in dig på tricken: reduktion modulo lämpligt tal, helst primtal, Gauss' lemma och Eisenstein (som båda kan bevisas genom sådan reduktion).

Vilka av följande polynom i $\mathbf{Q}[X]$ är irreducibla:

a) $f(X) = X^5 - 4X + 2$

b) $f(X) = X^4 + X^2 + X + 1$

c) $f(X) = X^4 - 10X^2 + 1$

d) $f(X) = X^5 - X^4 + 2X^3 + 1$

e) $f(X) = X^4 - 12X^3 + 9X^2 - 3$

(1 p per del, minus 1)

W 33)

a) p är ett primtal. Visa att

$$p|\binom{p}{k}, \quad 0 < k < p$$

b) Vi ska visa att *cirkeldelningspolynomet*

$$\Phi(X) = \frac{X^p - 1}{X - 1} \in \mathbf{Q}[X]$$

är irreducibelt. Det är inte så lätt. Mycket lättare är $\Phi(X + 1)$ som kan behandlas med kända metoder. Och det räcker. Varför? Gör!

(1+3 p)

Kroppar, utvidgningar, rotadjunktion

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.

W 34)

a) Avgör om polynomet $X^4 + X^2 + 2X + 1 \in K[X]$ är irreducibelt då $K = \mathbf{Q}$ resp. $K = \mathbf{Q}[i]$

(2 p)

b) Beskriv spaltningskroppen (över $\mathbf{Q}$) för polynomen

$$X^3 - 8; \quad X^4 - 4; \quad X^4 + 4X^2 + 4; \quad X^4 + X^3 + 2X^2 + X + 1; \quad X^6 - 4$$

. Den ska i samtliga fall beskrivas som delring av $\mathbf{R}$ eller $\mathbf{C}$.
(3 p)

W 35) Visa, som uppvärmning, att polynomen $X^2 - 3$, $\quad X^2 - 2X - 2$ har samma spaltningskropp (Visa hur det ena polynomet kan konstrueras ur det andra - i värsta fall ger dig själva rötterna en vink).
Visa därpå motsvarande påstående för polynomen

$$X^3 + 3X + 1, \quad X^3 + 3X^2 + 1, \quad X^3 - 3X^2 - 1, \quad X^3 + 3X - 1 \quad X^3 - 3X^2 + 6X - 3$$

(*utan att* lösa några ekvationer, tack!!!) (3 p)

W 36)

a) Är $\mathbf{Z}_7[X]/(X^2+1)$ en kropp? Bestäm minimalpolynomen och ordningen för $1+\alpha$, $2+3\alpha$, $3+\alpha$, där α är klassen av X modulo X^2+1.
b) Grundkropp nu, $k = \mathbf{Z}/(3)$, med tre element. Beskriv, och ange graden för, kroppsutvidgningar där polynomen $X^3 - 1$, $X^3 - X$, $X^4 - 1$, $X^9 - X$, $X^{27} - X$ samt $X^{12} - 1$ sönderfaller helt i förstagradsfaktorer. Utvidgningarna ska ges på formen $k[X]/(m(X))$, där $m(X)$ ska anges explicit.

(3+3 p)

W 37)

a) Polynomet $p(X) = X^3 + 9X + 6$ är irreducibelt över $\mathbf{Q}$, visa.
b) Bestäm minimalpolynomen (över $\mathbf{Q}$ för $1/\theta$, $1+\theta$ och $1/(1+\theta)$ (med ytterst korta räkningar!)
c) Bestäm, på polynomform, en invers till $1+\theta$. (1+1+1 p)

W 38) Visa att polynomet $X^4 - X + 1$ är irreducibelt över $\mathbf{Q}$. Låt θ vara en rot i en lämplig utvidgning. Bestäm minimalpolynomet för θ^2, över $\mathbf{Q}$.
(3 p)

W 39)

a) Ange de båda irreducibla polynomen av grad 2 över $k = \mathbf{Z}/(3)$, med högsta koefficient = 1), utöver X^2+1. Teorin utlovar att en kropp $K \supset k$ som innehåller en rot till ett av dessa polynom innehåller alla rötter till samtliga. Låt θ vara en rot till X^2+1. Uttryck alla rötter till alla tre polynomen som förstagradsuttryck i θ.
c) Beskriv, på lämpligt sätt, elementen i kroppen $K = \mathbf{Z_2}[X]/(X^2+X+1)$. Visa sedan att polynomet $T^4 + T + 1 \in K[T]$ är *reducibelt* över *denna* kropp men irreducibelt över $\mathbf{Z}_2$). (2+2 p)

W 40) Ange spaltningskroppen (och, speciellt, dess grad) för polynomet $X^6 - 1 \in \mathbf{Q}[X]$. (3 p)

W 41)

a) p är ett primtal, $k = \mathbf{Z}_p$. Vi betraktar polynomet $X^2 + aX + 1 \in k[X]$, låt θ vara en rot i kroppen $K \supset k$. Visa att θ^{p-1} eller θ^{p+1} är lika med ett.
b) När gäller det senare fallet?
c) Kan du ge exempel där $\theta^{(p+1)/2} = 1$?

(3 p)

b) Visa att polynomet $X^4 + 1$ är reducibelt i $\mathbf{Z}_p[X]$, $p = 3, 7, 13, 17$, och dela upp det i irreducibla faktorer. Man kan visa att polynomet ifråga är reducibelt modulo alla primtal. (3 p)

W 42)

a) Visa att $p(X) = X^6 + X^4 + X^2 + X + 1$ är irreducibelt över $\mathbf{Z}_2$. Är polynomet primitivt (dvs. kommer en rot att generera multiplikativa gruppen i utvidgningskroppen?)

b) Samma uppgift för $X^5 + X^2 + 1$. (2+2 p)

W 43)

a) Avgör om polynomen $X^3 + 2X + 1$ resp. $X^3 + 2X + 2$, $X^4 + X + 2$, $X^4 + X^3 + X^2 + X + 1$ i $\mathbf{Z}_3$ är irreducibla, resp. primitiva. Om något är imprimitivt, ange den multiplikativa ordningen för en rot i spaltningskroppen. (3 p)

W 44) Polynomet $X^4 + X + 1 \in \mathbf{Z}_2[X]$ är primitivt. Låt α vara en rot i en utvidningskropp med 16 element. Beräkna alla $1 + \alpha^j$ som potenser av α. Tips: ekvationen $\alpha^4 + \alpha + 1 = 0$ kan på flera sätt skrivas om i formen $1 + \alpha^j = \alpha^k$ Ur dessa samband kan ytterligare ett antal härledas, genom kvadrering. Sen finns inte så många möjligheter kvar.

Förklara sedan hur man med hjälp av det uträknade kan bestämma godtyckliga summor av två (eller flera) α–potenser. (2+1 p)

Konjugatklasser, normalisatorer, gruppers verkan

W 45)

a) Kubens vridningssymmetrier (en grupp G) kan ske kring tre olika typer av axlar: sådana som förbinder två hörn, mittpunkter på två sidor, samt tyngdpunkterna av två sidor. Sen finns ju också identiteten. Ange de möjliga vridningsvinklarna för varje typ av vridning (ledning: hur många grannhörn finns det till axelns ändpunkter?) och verifiera att gruppens ordning är 24.

Anm: Jag brukar visa a) på föreläsning, den ska då icke lämnas in.

b) Låt X vara mängden av rymddiagonaler i kuben. Antal? Verifiera att G verkar transitivt på X dvs. att till två godtyckliga diagonaler finns en vridning som överför den ena i den andra. Verifiera även att endast identiteten fixerar någon diagonal (dvs. att varje annan vridning rubbar åtminstone någon). Detta påvisar isomorfi med en känd grupp, vilken? !

c) Via en känd sats i böckerna ska du ur gruppens ordning, och antalet diagonaler, kunna bestämma ordningen av den delgrupp som stabiliserar en av diagonalerna. Gör det, och beskriv dess element!

d) Stabilisatorgruppen i c) innehåller en delgrupp av halva ordningen. Karakterisera på lämpligt sätt denna delgrupp och dess sidoklass. (1+1+1+1 p)

W 46) (fyra delar)

x, g är permutationer.

Böckerna har satser som ger en enkel beskrivning av konjugatet xgx^{-1} när cykelstrukturen av g är känd.

a) Visa att $g = (12)(34)$ och $h = (13)(24)$ är konjugerade i S_4. Bestäm alla lösningar till $xgx^{-1} = h$. Är g, h konjugerade som element i A_4?

b) Samma uppgift för permutationerna $(1\,2\,3)$ och $(2\,3\,4)$

c) Anta att centralisatorn H till $g \in G$ är känd och att vi vet *en* lösning till $xgx^{-1} = h$. Visa att vi då känner alla.

d) Bestäm antalet element i S_6 som kommuterar med $(12)(345)$ Beskriv dem också!

(2+2+2+2 p)

W 47)

a) Bestäm antalet element i S_n som kommuterar med (12),$(12)(34)$ resp. $(1\,2 \ldots n)$. Beskriv dem.

b) Bestäm antalet element i S_6 som har cykelstrukturen $(abc)(def)$, dit speciellt $\sigma_1 \cdot \sigma_2 = (123)(456)$ hör. Bestäm härur antalet element som kommuterar med detta element. Visa att $\sigma_1^m \sigma_2^n$ hör dit. Hur många är dessa element? Ange ytterligare ett och använd det till att bestämma alla.

(3 p)

W 48) Låt $f(x_1, x_2, \ldots, x_n)$ vara ett polynom i n variabler. Vi definierar $g = f^\sigma, \sigma \in S_n$ genom

$$g(x_1, x_2, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

T ex är $(x_1x_2)^{(1\,2)} = x_2x_1 = x_1x_2$ och $(x_1 - x_2)^{(1\,2)} = x_2 - x_1$.

Vi säger att σ *fixerar* f om $f^\sigma = f$. Vi säger att en delgrupp av S_n fixerar f om alla element gör det.

Man verifierar lätt att $p^{(\sigma\tau)} = (p^\tau)^\sigma$ (tyvärr - man borde använda inversen för att ordningen ska bli "rätt"!).

a) Visa att de permutationer som fixerar ett givet f bildar en delgrupp H av S_n. När gäller att $f^\sigma = f^\tau$?

b) Beskriv den delgrupp av S_3 som fixerar $(x_3 - x_1)(x_3 - x_2)(x_2 - x_1)$. Hur verkar övriga element? Generalisera dina iakttagelser till S_n.

c) Beskriv den delgrupp H av S_4 som fixerar $f = (x_1 - x_2)(x_3 - x_4)$. Ange också alla möjliga f^σ och relatera antalet till H:s index i S_4

d) Samma uppgift för $f = (x_1 + x_2)(x_3 + x_4)$ och $f = x_1x_3 + x_2x_4$

e) Ange ett homogent fjärdegradspolynom som fixeras av $(13), (1234) \in S_4$ men inte av hela S_4 (slut, således, att de båda permutationerna inte genererar S_4.) Verifiera detta gärna även direkt!

$(5 \cdot 1$ p)

W 49) . I samtliga uppgifter nedan ska arrangemang och färgningar identifieras om de övergår i varandra genom symmetrigruppens verkan, dvs. om de tillhör samma bana.

a) Vi har ett kvadratiskt bräde, med 3×3 rutor, och vill färga fem rutor vita, de övriga svarta. På hur många sätt kan detta göras, med hänsyn tagen till i) kvadratens åtta symmetrier, ii) de fyra vridningarna? Ge exempel på två färgningar som identifieras i det första fallet, men inte i det andra. (3 p)

c) Antalet sätt att färga de 6 kanterna i en regelbunden tetraeder med 3 färger, av vilka inte samtliga behöver användas. (3 p)

Bestäm först, förstås, de 12 vridningarna.

d) Samma som c), men kub. Det finns 24 vridningar.

e) Ett bräde med 16 rutor ska färläggas med två färger. Hur många sätt blir det, med hänsyn till kvadratens åtta symmetrier? (2 p)

f) Liksidig triangel, 5 färger, minst 2 ska användas. (3 p)

h) Kvadrat, 4 färger, likhet tillåten.

i) Som c) men hörn istf. kanter. (c + 2p)

j) Som c, men alla färger ska användas. (c + 2p)

k) Regelbunden p–hörning, p primtal, r stycken färger. Härled, på köpet, Fermats Lilla Sats.

(3 p)

Du lämnar högst 2 av dessa (eller vad programmet anger), men givetvis inte någon uppgift som står i den bok du valt.

Kinesiska Restsatsen, Lineär Rekursion

W 50) Ange alla lösningar till kongruenssystemet

$$\begin{aligned} n &\equiv 1 \pmod 7 \\ n &\equiv 2 \pmod 8 \\ n &\equiv 3 \pmod 9 \end{aligned}$$

(1 p)

W 51)

a) Visa att

$$\begin{aligned} x &\equiv a_1 \bmod m_1 \\ x &\equiv a_2 \bmod m_2 \end{aligned}$$

är lösbar om, och endast om, $(m_1, m_2)|(a_1 - a_2)$. Bestäm alla lösningar till

$$\begin{aligned} x &\equiv 7 \bmod 10 \\ x &\equiv 12 \bmod 15 \end{aligned}$$

b) Anta att heltalet m innehåller r olika udda primfaktorer. Faktorn 2 kan ingå, och alla faktorer kan ingå med multiplicitet. För t ex. $m = 150$ är $r = 2$, eftersom de udda primfaktorerna är 3 och 5.
Visa, att det finns minst 2^r lösningar till kongruensen $x^2 \equiv 1 \pmod m$, t ex genom att studera r stycken enklare kongruenser.

c) Bonus: Visa att det finns fler om m är delbart med 8. (2+2+1 p)

W 52) Lös kongruenssystemet

$$\begin{aligned} f(X) &\equiv X \pmod{(X-1)^2} \\ f(X) &\equiv X + 1 \pmod{(X+1)^2} \end{aligned}$$

i $\mathbf{Q}[X]$. (3 p)

W 53)

a) Beskriv $\mathbf{Z}_{30}$ som direkt summa (produkt) av tre kroppar $\mathbf{Z}_{30} \simeq K_1 \oplus K_2 \oplus K_3$. Förklara härur varför maximala ordningen av ett invertibelt element är 4.

b) Visa att även $\mathbf{Z}_{385}$ är direkt summa av kroppar (vad är det väsentliga med talsom 30 och 385?). Använd detta till att bestämma maximala ordningen
av ett invertibelt element. (2+2 p)

W 54) Visa att $\mathbf{Z}_2[X]/(X^5 + X + 1)$ är en direkt summa (produkt) av två kroppar. Ange idempotenterna explicit. (2 p)

W 55)

a) Studera II.2. i stencilen om C.R.T. Visa att varje summa av olika idempotenter e_i är en idempotent. Finns det andra?
b) Beskriv en direktsumma-uppdelning av ringen $\mathbf{Z}/(504)$ i ringar av typen $\mathbf{Z}/(p^n)$, där p är primtal. Beskriv speciellt idempotenterna och hur en godtycklig restklass modulo 504 kan uttryckas i dessa.
c) $k = \mathbf{Z}/(2)$. Visa att polynomen $x^j + x + 1$, $j = 2, 3, 4$ är irreducibla. Beskriv C.R.T-uppdelningen av ringen $k[X]/(f_1 f_2 f_3)$ analogt uppgift b). Kontrolltips: matlab:s kommandon *conv, deconv, mod.*
(2+2+2 p)

W 56) Bestäm ett polynom $f(x) \in \mathbf{Q}[X]$ av grad högst $= 3$, med $f(-1) = 1, f(1) = -1, f'(-1) = -1, f'(1) = 1$! Förklara teoretiskt varför systemet säkert är lösbart för godtyckliga högerled.

W 57)
a) Lös rekursionen $s_0 = 0, s_1 = 1, s_{n+2} - 5s_{n+1} + 6s_n = 0$ i karakteristik 0.
b) Lös rekursionen $s_0 = 0, s_1 = 0, s_2 = 1; \quad s_{n+3} - s_{n+2} - 8s_{n+1} + 12s_n = 0$ i karakteristik 0.
(3 p)

W 58) Anta visat att $X^9 + X + 1$ är irreducibelt över $\mathbf{Z}_2$. Bestäm maximala perioden för en lösning till rekursionen $s_{n+9} + s_{n+1} + s_n = 0$, $n \geq 0$.
(3 p)

W 59) Lös rekursionen
$$a(n+2) - 3a(n+1) + 2a(n) = 2^n,$$
med begynnelsevillkoren $a(0) = 0, a(1) = 1$. Karakteristik 0.
(3 p)