Oppgave 2. (a) Vi skal vise at $H^* = \left\{ 0 \neq \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \mid a, b \in \mathbb{C} \right\}$ er en gruppe under matrisemultiplikasjon. Vi har at det $\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} = a\bar{a} + b\bar{b} = |a|^2 + |b|^2 > 0$ da enten $a \neq 0$ eller $b \neq 0$. Dette fører til at $H^* \subset K = \{$inverterbare 2×2 matriser over $\mathbb{C}\}$. Vi veit at K er en gruppe under matrise-multiplikasjon, og ønsker å vise at H^* er en undergruppe av K:

(i) La $\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}, \begin{pmatrix} a' & b' \\ -\bar{b'} & \bar{a'} \end{pmatrix} \in H^*$.

$$\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \begin{pmatrix} a' & b' \\ -\bar{b'} & \bar{a'} \end{pmatrix} = \begin{pmatrix} aa' - b\bar{b'} & ab' + b\bar{a'} \\ -\bar{b}a' - \bar{a}\bar{b'} & \bar{a}\bar{a'} - b'\bar{b} \end{pmatrix}$$

som er med i H^* siden $aa' - b\bar{b'}, ab' + b\bar{a'} \in \mathbb{C}$ da $a, b \in \mathbb{C}$ og $-\bar{b}a' - \bar{a}\bar{b'}$ er den negative av den komplekskonjugerte av $ab' + b\bar{a'}$ og $\bar{a}\bar{a'} - b'\bar{b}$ er den komplekskonjugerte av $aa' - b\bar{b'}$.

(ii) $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ er identites elementet i K, og $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in H^*$

(iii) La $\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \in H^*$. Da er $\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}^{-1} = 1/\delta \begin{pmatrix} \bar{a} & -b \\ \bar{b} & a \end{pmatrix}$ som er med i H^* siden $\overline{(\frac{\bar{a}}{\bar{b}})} = \frac{a}{\bar{a}}$ og $-(-\frac{\bar{b}}{\bar{a}}) = \frac{\bar{b}}{\bar{a}}$.

(b) Vi skal finne undergruppen G av H^* generert av $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ og $B = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$. En undergruppe generert av A og B er per definisjon minste undergruppe som inneholder A og B. G må altså inneholde identitets element I, A, B og alle mulige produkt av A og B. Spesielt, må G inneholde alle potenser av A og B, så la oss begynne med å se på dem.

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ A^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},\ A^3 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},\ A^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$B = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},\ B^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},\ B^3 = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix},\ B^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Altså, så langt har vi funnet 6 elementer i G: I, A, A^2, A^3, B og B^3.

$AB = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$ og $BA = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ må vi også ha i G. Det er gitt at G har 8 elementer så vi trenger ikke å lete etter flere. Elementene i G er altså:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},$$

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

(c) Er G isomorf med D_4? Også her er det enklest å se på orden til elementer først. Hvis orden til elementene i de to gruppene ikke skulle stemme overens, da kan vi si at de ikke er isomorfe.

Etter litt regning finner vi ut at alle elementene i G bortsett fra I og A^2 har orden 4. I D_4 er det bare to elementer av orden 4. Dermed kan G ikke være isomorf med D_4.

Oppgave 5. (a) Vi skal finne alle irredusible polynom av grad 5 over $\mathbb{Z}_2$. Et polynom $f(x)$ av grad 5 over $\mathbb{Z}_2$ er på formen $f(x) = a_o + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5$, hvor $a_0, \ldots, a_5 \in \mathbb{Z}_2$. Vi leter etter polynom av grad 5, så a_5 må være lik 1. Videre, hvis $a_0 = 0$ er $x = 0$ en rot i polynomet og polynomet er dermed redusibelt, så a_0 må i hvertfall være forskjellig fra 0 i et irredusibelt polynom. Altså,

$$f(x) = 1 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + x^5, \text{ for } \mathrm{a}_1, \ldots, \mathrm{a}_4 \in \mathrm{Z}_2$$

så vi leter etter irredusible polynom blant 16 mulige. La oss i stedet prøve å finne redusible polynom blant dem. Hvis $f(x)$ er redusibelt, så er det enten produkt av et lineart polynom og et polynom av grad 4 eller produkt av et irredusibelt polynom av grad 2 og et irredusibelt polynom av grad 3.

- Anta $f(x) = (x + b)g(x)$ der $g(x)$ er et polynom av grad 4: $g(x) = c_0 + c_1x + c_2x^2 + c_3x^3 + x^4$. Siden konstantleddet i $f(x)$ er forskjellig fra 0, må både $b \neq 0$ og $c_0 \neq 0$, altså, $b = c_0 = 1$. Da står vi med 8 mulige valg av trippelet (c_1, c_2, c_3) ($c_i \in \mathbb{Z}_2$!). Hvert trippel gir oss et polynom av grad 4 og (multiplisert med $(x + 1)$) et redusibelt polynom av grad 5.
  - (0,0,0): gir polynomet $f_1(x) = x^5 + x^4 + x + 1$
  - (1,0,0): $f_2(x) = x^5 + x^3 + x + 1$
  - (0,1,0): $f_3(x) = x^5 + x^4 + x^3 + x^2 + x + 1$
  - (0,0,1): $f_4(x) = x^5 + x^4 + x^2 + 1$
  - (1,1,0): $f_5(x) = x^5 + x^2 + x + 1$
  - (1,0,1): $f_6(x) = x^5 + x^3 + x^2 + 1$
  - (0,1,1): $f_7(x) = x^5 + x^4 + x^3 + 1$
  - (1,1,1): $f_8(x) = x^5 + 1$

  Så her har vi fått 8 reduktible polynom av grad 5.
- Anta at $f(x) = g(x)h(x)$ der $g(x)$ er et irredusibelt polynom av grad 2 og $h(x)$ et irredusibelt polynom av grad 3. Det er bare ett irredusibelt polynom over $\mathbb{Z}_2$ av grad 2, nemlig $x^2 + x + 1$, så $g(x)$ må være dette polynomet. Det er to irredusible polynom av grad 3 over $\mathbb{Z}_2$, altså to muligheter for $h(x)$: $h_1(x) = x^3 + x^2 + 1$ og $h_2(x) = x^3 + x + 1$. Dermed får vi to nye redusible polynom av grad 5:
  - $f_9(x) = g(x)h_1(x) = x^5 + x + 1$
  - $f_{10}(x) = g(x)h_2(x) = x^5 + x^4 + 1$

I alt har vi fått at 10 av de 16 mulige polynom av grad 5 er redusible. De øvrige er irredusible:

- $f_{11} = x^5 + x^4 + x^3 + x^2 + 1$
- $f_{12} = x^5 + x^4 + x^3 + x + 1$
- $f_{13} = x^5 + x^4 + x^2 + x + 1$
- $f_{14} = x^5 + x^3 + x^2 + x + 1$
- $f_{15} = x^5 + x^3 + 1$
- $f_{16} = x^5 + x^2 + 1$

(b) Ta ett irredusibelt polynom av grad 5 over $\mathbb{Z}_2$, ett av de vi har funnet i (a), for eks. $f_{16} = x^5 + x^2 + 1$. Det er irredusibelt og dermed er $< f_{16} >$ et maksimalt ideal, noe som medfører at $\mathbb{Z}_2[x]/ < f_{16} >$ er en kropp.

La oss sjekke hvor mange elementer det er i $\mathbb{Z}_2[x]/ < f_{16} >$. Vi vet at

$$\mathbb{Z}_2[x]/ < f_{16} >= \{a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 | a_0, a_1, a_2, a_3, a_4 \in \mathbb{Z}_2\}$$

I og med at koeffisientene a_0, a_1, a_2, a_3, a_4 er fra $\mathbb{Z}_2$ er det klart at $\mathbb{Z}_2[x]/ < f_{16} >$ har $2^5 = 32$ elementer.

(c) Vi skal finne kjernen til $\phi : \mathbb{Z}_2[x] \to \mathcal{M}_5(Z_2)$ gitt ved $\phi(f) = f(A)$.

Vi vet at kjernen til en ringhomomorfi (det er underforstått i teksten at ϕ er en ringhomomorfi) $\phi : R_1 \to R_2$ er et ideal i R_1. Videre vet vi at alle ideal i $\mathbb{Z}_2[x]$ er generert av bare ett element, altså på formen $< g(x) >$ for et element $g(x) \in \mathbb{Z}_2[x]$.

For å finne kjernen til ϕ, må vi altså finne et polynom $g(x) \in \mathbb{Z}_2[x]$ av laveste grad slik at $g(A) = 0$ (med 0 menes 0-matrisa i $\mathcal{M}_5(Z_2)$ her) og da er $\text{Ker}\phi =< g(x) >$. Betrakt

$$I = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, A = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}, A^2 = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

$$A^3 = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}, A^4 = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{pmatrix}, A^5 = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

Etter en del prøving og feiling (husk at vi er i $\mathbb{Z}_2 = \{0, 1\}$!) finner vi ut at ingen polynom $g(x)$ av grad 2 i $\mathbb{Z}_2[x]$ kan oppfyllet kravet om at $g(A) = 0$ og ingen polynom av grad 3 eller 4 heller. Vi finner derimot at $g(x) = x^5+x^3+x^2+x+1 \in \mathbb{Z}_2[x]$ er slik at $g(A) = 0$. Siden $g(x)$ er av laveste grad slik at det er oppfylt følger det at $\text{Ker}\phi =< g(x) >$ der $g(x) = x^5 + x^3 + x^2 + x + 1$.

Merk: $g(x)$ er minimal polynomet til matrisa A og minimal polynomet til en matrise går opp i det karakteristiske polynomet til matrisa. Så, for å finne $g(x)$ kunne vi finne det karakteristiske polynomet til A, legge merke til at det er et irredusibelt polynom (sammenligne med de fra (a)) og konkludere at i dette tilfelle må det minimale polynomet være lik det karakteristiske, $g(x)$.

Fra Fundamental teorem for ringhomomorfier har vi at

$$\text{Im}\,\phi \cong Z_2[x]/\,\text{Ker}\,\phi$$

I (a) har vi funnet ut at $g(x) = x^5 + x^3 + x^2 + x + 1$ er et irredusibelt polynom. Det medfører av $\text{Ker}\phi =< g(x) >$ er et maksimalt ideal, noe som igjen medfører at $Z_2[x]/\,\text{Ker}\,\phi$ er en kropp. Imϕ er isomorf med $\mathbb{Z}_2[x]/\,\text{Ker}\,\phi$ og er dermed også en kropp.

Imϕ må også ha samme antall elemener som $\mathbb{Z}_2[x]/\,\text{Ker}\,\phi$, så la oss sjekke hvor mange elementer det er i $\mathbb{Z}_2[x]/\,\text{Ker}\,\phi$. Vi vet at

$$\mathbb{Z}_2[x]/\,\text{Ker}\,\phi = \{a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 | a_0, a_1, a_2, a_3, a_4 \in \mathbb{Z}_2\}$$

I og med at koeffisientene a_0, a_1, a_2, a_3, a_4 er fra $\mathbb{Z}_2$ er det klart at $\mathbb{Z}_2[x]/\,\text{Ker}\,\phi$ har $2^5 = 32$ elementer og følgelig er Imϕ en kropp med 32 elementer.

Eksamen i MNFMA205/SIF5021, 5. des.2000-Løsningsforslag

Oppgave 3. (a) La oss kalle en av steinene på den øverste randen 1, den som står til venstre til 1 kaller vi 2, 3 den som er til venstre til 2 osv til 6. La oss kalle steinen som er under 1 (på nederste randen)7, den til venstre til 7 kaller vi 8, osv. til 12. Merk nå at ved å rotere armbåndet i rommet kan vi få 1 over til posisjon av alle steinene $1, \ldots, 12$, og gruppen av symmetrier på armbåndet G består av akkurat disse bevegelsene. Det er dermed 12 elementer i G. La oss skrive opp elementene i G som produkter av disjunkte sykler.

- 1 til 1: identitet. La oss kalle det g_{11}
- 1 til 2: La oss kalle dette elementet $g_{1,2}$. $g_{1,2} = (1, 2, 3, 4, 5, 6)(7, 8, 9, 10, 11, 12)$
- 1 til 3: $g_{1,3} = (1, 3, 5)(2, 4, 6)(7, 9, 11)(8, 10, 12)$
- 1 til 4: $g_{1,4} = (1, 4)(2, 5)(3, 6)(7, 10)(8, 11)(9, 12)$
- 1 til 5: $g_{1,5} = (1, 5, 3)(2, 6, 4)(7, 11, 9)(8, 12, 10)$
- 1 til 6: $g_{1,6} = (1, 6, 5, 4, 3, 2)(7, 12, 11, 10, 9, 8)$
- 1 til 7: $g_{1,7} = (1, 7)(2, 12)(3, 11)(4, 10)(5, 9)(6, 8)$

- 1 til 8: $g_{1,8} = (1,8)(2,7)(3,12)(4,11)(5,10)(6,9)$
- 1 til 9: $g_{1,9} = (1,9)(2,8)(3,7)(4,12)(5,11)(6,10)$
- 1 til 10: $g_{1,10} = (1,10)(2,9)(3,8)(4,7)(5,12)(6,11)$
- 1 til 11: $g_{1,11} = (1,11)(2,10)(3,9)(4,8)(5,7)(6,12)$
- 1 til 12: $g_{1,12} = (1,12)(2,11)(3,10)(4,9)(5,8)(6,7)$

Altså, $G = \{g_{1,k} | k = 1, \ldots, 12\}$.

(b) La X være mengden av alle mulige armbånd vi kan lage med tre typer steiner til disoposisjon (tenk deg at armbåndet står fast). Det er 3^{12} elementer i X (vi velger en blant 3 mulige for hver stein $1, \ldots, 12$). Men, armbåndet står egentlig ikke fast, det kan roteres i rommet, og to armbånd er like hvis vi kan rotere det ene til å være lik det andre. Så, antall forskjellige armbånd det er mulig å lage er lik antall orbiter i X under virkning av gruppe G. Så, la oss bruke Burnside's formel for å finne antal orbiter r:

$$r = \frac{1}{|G|}(|X_{g_{1,1}}| + \cdots + |X_{g_{1,12}}|)$$

- $|X_{g_{1,1}}| = |X| = 3^{12}$
- $|X_{g_{1,2}}| = 3^2$ (siden $g_{1,2}$ er produkt av 2 disjunkte sykler)
- $|X_{g_{1,3}}| = 3^4$ ($g_{1,2}$ er produkt av 4 disjunkte sykler)
- $|X_{g_{1,4}}| = 3^6$
- $|X_{g_{1,5}}| = 3^4$
- $|X_{g_{1,6}}| = 3^2$ og
- $|X_{g_{1,k}}| = 3^6$ for all $k = 7, \ldots, 12$.

Dermed er

$$r = \frac{1}{12}(3^{12} + 2 \cdot 3^2 + 2 \cdot 3^4 + 7 \cdot 3^6) = 44727$$

antall forskjellige armbånd gullsmeden kan lage.

Oppgave 4. (a) Vi skal vise at orden til G er $(p^2-1)(p^2-p)$, der G er mengden av 2×2-matriser over $\mathbb{Z}_p$ med determinant forskjellig fra 0 (det er underforstått fra teksten at G er en gruppe under vanlig matrisemultiplikasjon i $\mathbb{Z}_p$)

For at $\det\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ skal være forskjellig fra 0 (der $a, b, c, d \in \mathbb{Z}_p$), må "vektorene" $(a,b), (c,d) \in \mathbb{Z}_p \times \mathbb{Z}_p$ være lineært uavhengige.

Antall måter å velge den første vektor, (a,b) er $p^2 - 1$: vi kan velge hvilket som helst par fra $\mathbb{Z}_p \times \mathbb{Z}_p$ (p^2 mulige) bortsett fra (0,0). Altså: $p^2 - 1$.
Det er p vektorer i $\mathbb{Z}_p \times \mathbb{Z}_p$ som er lineært avhengige av den utvalgte (a,b): de som er gitt ved $u(a,b), u \in \mathbb{Z}_p$. Når vi skal velge (c,d) kan vi velge blant p^2 elementer i $\mathbb{Z}_p \times \mathbb{Z}_p$ unntatt disse p vektorer.

Så, alt i alt, vi har $p^2 - 1$ valg for den første vektoren og $p^2 - p$ valg for den andre for hver av disse. Det er dermed $(p^2-1)(p^2-p)$ elementer i G.

(b) Definer $f : G \to \mathbb{Z}_p^*$ ($\mathbb{Z}_p$ under multiplikasjon modulo p, $\mathbb{Z}_p^* = \mathbb{Z}_p - \{0\}$) ved at $f(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) = \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{Z}_p$.

Det er lett å sjekke at f er en gruppe homomorfi:

$$f(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}) = \det(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix})$$

$$= \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \det \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = f(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) f(\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix})$$

f er på: gitt $x \in \mathbb{Z}_p^*$, da er $\begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix}$ med i G og

$$f(\begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix}) = x$$

Merk at Ker$f = H$. Ved å bruke Fundamental teoremet for gruppe homomorfi, får vi at

$$G/H \cong \mathbb{Z}_p^* \text{og dermed er } |\mathrm{H}| = \frac{|\mathrm{G}|}{|\mathbb{Z}_\mathrm{p}^*|} = \frac{(\mathrm{p}^2-1)(\mathrm{p}^2-\mathrm{p})}{\mathrm{p}-1} = \mathrm{p}(\mathrm{p}^2-1)$$

(c) Vi skal vise at

$$T = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} | b \in \mathbb{Z}_p \right\}$$

er en Sylow p-undergruppe av H.

La oss først vise at T er en undergruppe av H: Det et klart at $T \subseteq H$.

1. H lukket: Gitt $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & b' \\ 0 & 1 \end{pmatrix} \in T$. Da er

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b+b' \\ 0 & 1 \end{pmatrix}$$

med i T siden $b + b' \in \mathbb{Z}_p$ når $b, b' \in \mathbb{Z}_p$.

2. $I \in T$: Identitets elementet i H, $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, er åpenbart med i T.

3. Inversen til hvert element: Gitt $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in T$. La $-b$ stå for inversen til b i $(\mathbb{Z}_p, +_p)$. Da er $\begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix} \in T$ og

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Altså, for hvert element i T er dets invers også med i T.

Merk: Orden til H er $|H| = p(p-1)(p+1)$, så en Sylow-p-undergruppe har p elementer (p går ikke opp i hverken $p-1$ eller $p+1$).

La $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in T$.

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}^r = \begin{pmatrix} 1 & rb \\ 0 & 1 \end{pmatrix}$$

Så, orden til $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ er lik orden til b i $(\mathbb{Z}_p, +_p)$. Da p er et primtall, orden til hvert element forskjellig fra identitets elementet i $(\mathbb{Z}_p, +_p)$ er p og dermed er orden til hvert element i T (bortsett fra identitets elementet I) også p og T er følgelig en p-undergruppe av H. Siden $|T| = p$, er det da en Sylow-p-undergruppe av H.

(d) Hvor mange Sylow-p-undergrupper har H?

Tredje Sylow teorem: Antall r av Sylow-p-undergupper i en gruppe er $r \equiv 1 (\mathrm{mod}\, p)$ og går opp i orden til gruppa.

I vårt tillfelle må r altså være kongruent med 1 modulo p og gå opp i $|H| = p(p-1)(p+1)$, så r kan være enten 1 eller $p+1$.

Andre Sylow teorem gir at Sylow-p-undergrupper er konjugerte av hverandre, så hvis T er eneste Sylow-p-undergruppe i H, må den være normal. Men, T er ikke

normal: ta for eksempel $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in T$ og $\begin{pmatrix} 0 & 4 \\ 1 & 0 \end{pmatrix} \in H$.

$$\begin{pmatrix} 0 & 4 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 4 \\ 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix} \notin T$$

Da kan T ikke være normal og følgelig ikke den eneste Sylow-p-undergruppe i H. Dermed har vi kommet frem til at det er $p+1$ Sylow-p-undergrupper i H.