Om multiplikativa gruppen i en ändlig kropp

Gruppen i rubriken är cyklisk. Böckernas bevis går omvägen över en stor och allmän teori för abelska grupper, vilken inte vår kurs kan härbärgera. Därför ger jag ett mer direkt bevis. Väsentligt är att polynomekvationer över en kropp har högst så många rötter som graden anger.

Vi formulerar satsen en aning allmännare:

Sats. *Låt K vara en kropp. Låt G vara en ändlig delgrupp av multiplikativa gruppen*

$$K^* =< K - \{0\}, \cdot >$$

. Det gäller att G är cyklisk.

Exempel. Följande exempel ska vara känt från Analysen.

Vi låter $K = \mathbf{C}$ och G lika med lösningsmängden till ekvationen $X^d = 1$. Denna är en grupp, ty det finns en etta, produkten av två rötter är ånyo en rot och om a är en rot så är a^{d-1} dess invers.

I Analysen visas att denna grupp består av potenserna $\alpha^k, k = 0, 1, \ldots, d-1$ av

$$\alpha = e^{2\pi \cdot i/d};$$

som är roten med minsta positiva argument. I detta fall bekräftar satsen något vi redan vet.

För övrigt måste varje ändlig delgrupp av $K = \mathbf{C}^*$ bestå av lösningar till $X^d = 1$, där d är gruppens ordning.

Ordningen av en generator måste också vara gruppens ordning och av detta sluter man sig till lösningsmängderna till de binomiska ekvationerna $X^e = 1$ är de *enda* ändliga delgrupperna av $\mathbf{C}^*$.[]

Exempel. I kursens inledning introduceras, som första exempel på ändliga kroppar, restklassringarna $\mathbf{Z}_p$, där p är ett primtal. För t ex $p = 7$ kontrollerar man lätt att klassen [2] har ordning 3, och alltså inte genererar multiplikativa gruppen (som ju har ordning 7-1=6). Däremot gäller:

$$[3]^2 = [9] = [2] \neq [1]$$

$$[3]^3 = [27] = [6] \neq [1]$$

Ordningen av [3] är varken 6/3=2 eller 6/2=3 och måste alltså vara 6. Där har vi en generator.[]

Låga exempel kan lura en att tro att generatorer alltid är förhållandevis små. Men t ex för $p = 1399$ är minsta positiva generatorn lika med 13.

Nu bevisar vi satsen.

Bevis. Låt $m = |G|$ vara gruppens ordning. Låt $p_i, i = 1, 2, \ldots k$ vara primfaktorerna. För en godtycklig av dem kan vi skriva:

$$m = p_i^{e_i} \cdot q_i \text{ där } e_i > 0 \text{ och } (p_i, q_i) = 1.$$

Ekvationen

$$X^{m/p_i} = 1$$

har högst $m/p_i < m$ rötter. Låt $x_i \in G$ vara en icke-rot. Eftersom ordningen av x_i delar $m = p_i^{e_i} \cdot q_i$ men inte m/p_i, måste den vara delbar med hela p_i- potensen $p_i^{e_i}$,

$$o(x_i) = p_i^{e_i} \cdot r_i, \quad (p_i, r_i) = 1$$

För

$$y_i = x_i^{r_i}$$

gäller då att

$$y_i^{p_i^{e_i}} = 1$$

så ordningen är en faktor i $p_i^{e_i}$. Men det kan inte gälla att någon lägre potens

$$y_i^{p_i^{f_i}} = 1, \quad f_i < e_i$$

ty då vore

$$x_i^{p_i^{f_i} r_i} = 1$$

vilket är en lägre potens än ordningen av x_i.

Således har våra y_i de relativt prima ordningarna $p_i^{e_i}$. Deras produkt måste då enligt följande lemma (använt flera gånger) ha ordning lika med produkten av dessa ordningar, dvs. ordningen av $y_1 \cdot y_2 \cdots y_k$ är lika med m.

Lemma. *Anta att g, h är kommuterande element i en grupp G, vilkas ordningar r, s är relativt prima. Då är ordningen av gh lika med produkten rs*

Bevis. Vi har

$$(gh)^{rs} = (g^r)^s \cdot (h^s)^r = e^s \cdot e^r = e$$

så ordningen av gh är en faktor i rs. Vi behöver visa den omvända delbarheten.

Anta således

$$(gh)^d = g^d \cdot h^d = e$$

Höj sambandet till r:–e potens:

$$e = e^d = (g^r)^d \cdot h^{dr} = h^{dr}$$

dr är alltså en multipel av h:s ordning s.

Eftersom r, s är relativt prima följer enligt en klassisk delbarhetssats att $s|d$.

Genom att istället höja sambandet till s:e potens visar vi på samma sätt att $r|d$.

Eftersom r, s är relativt prima visar ännu en klassisk delbarhetssats att dessa båda delbarheter medför $rs|d$ vilket var den eftersökta omvända delbarheten.[]