# .I Karakteristik

**.I.1 Sats.** *Låt $K$ vara en ändlig kropp. $K$ innehåller då en minsta delkropp $k$, bestående av alla upprepade summor av ettan: $0, 1, 2 \cdot 1 = 1 + 1, 3 \cdot 1 = 1 + 1 + 1, \ldots, p \cdot 1 = 0, \ldots$. $k$ är isomorf med $\mathbf{Z}_p$ där $p$ är ett primtal. $p$, som är additiva ordningen för alla nollskilda element, kallas för $K$:s* **karakteristik**. *$k$ är dess* **primkropp**.

Satsen bevisas i alla böcker, t ex genom att man bildar en uppenbar homomorfism från $\mathbf{Z}$ till $K$ och bestämmer dess kärna. ∎

**.I.2 Sats. Linus Dröm (Freshman's Dream)**:

*Låt $K$ vara en ändlig kropp av karakteristik $p$. För godtyckliga element $a, b \in K$ gäller då att*

$$(a \pm b)^p = a^p \pm b^p$$

$$(a + b)^{p^n} = a^{p^n} \pm b^{p^n}$$

Bevisas också i alla böcker. Första delen följer av att

$$p | \binom{p}{m} = \frac{p!}{m!(p-m)!}, \quad m = 1, 2, \ldots, p-1$$

eftersom täljaren innehåller primfaktorn $p$ som inte kan förkortas bort. Den andra delen följer ur den första genom upprepning (induktion). I fallet $p = 2$ ska man observera att plus och minus är samma sak, eftersom $a + a = (1+1)a = 0 = a - a$. ∎

**.I.3 Sats.** *$K$ ändlig kropp, $k$ dess primkropp. $k$ består då av rötterna till $X^p - X \in k[X]$*

**Bevis:** Att alla element $a \in k$ uppfyller $a^p - a = 0$ är inget annat än lilla Fermat. Eftersom ett polynom över en kropp kan ha högst så många rötter som gradtalet anger, så finns inga fler rötter än dessa. ∎

**.I.4 Sats.** *$K$ ändlig kropp, $k$ dess primkropp. Betrakta polynomet $X^{p^n} - X \in k[X]$ och dess rötter i $K$ (som kan vara färre än $p^n$). Dess bildar då en delkropp $L$ av $K$. Speciellt gäller att en spaltningskropp till $X^{p^n} - X \in k[X]$* består av dess rötter.

**Bevis:** Sätt $q = p^n$ Låt $a, b \in L$, dvs. $a^q = a, b^q = b$. Då är $(a \pm b)^q = a^q \pm b^q = a \pm b$, det första enligt Linus Dröm.

Så även $a \pm b \in L$, dvs. $L$ är sluten under addition och subtraktion.

Vidare är $(a \cdot b^{\pm 1})^q = a^q \cdot (b^q)^{\pm 1} = a \cdot b^{\pm 1}$, så att även $a \cdot b^{\pm 1}$ tillhör rotmängden $L$.

Detta visar slutenheten under multiplikation och division.

∎

*Anm*: Ekvationen $X^{p^n} - X = 0$ har åtminstone $p$ rötter, nämligen elementen i primkroppen. Av $a^p = a$ följer nämligen $a^{p^2} = a^p = a$ osv.

Om t ex $K$ har $p^3$ element, och $n = 2$, finns inte fler rötter än så. Man kan nämligen visa att $X^{p^m} - X$ och $X^{p^n} - X$ är relativt prima om $m, n$ är det.

Det gäller tillochmed att

$$(X^{p^m} - X, X^{p^n} - X) = X^{p^d} - X$$

om $(m, n) = d$. Detta kan visas med kroppsteoretiska, gruppteoretiska, eller helt elementära, metoder. Fallet $m|n$ behandlas i dokumentet om "universalpolynomet".

## .II Satser om ändliga kroppar: existens och entydighet.

$k$ är kroppen $\mathbf{Z}_p$, av karakteristik $p$. Den allmänna teorin för ändliga kroppar $K$ av karakteristik $p$ kan sammanfattas i följande tre satser

**.II.1 Sats. Existenssatsen**

*En spaltningskropp, över $k$, till polynomet $X^{p^n} - X$, har precis $p^n$ element, och består av dess rötter (dessa är speciellt således olika).*

**.II.2 Sats. Entydighetssatsen**

a) *Varje kropp med $p^n$ element har formen $K = k[\theta]$, där $\theta \in K$,*
b) *$K$ är isomorf med en kvotkropp $k[X]/(m(x))$ där $m(X)$ (minimalpolynomet till $\theta$ i föregående del) är en irreducibel faktor i $X^{p^n} - X$, av grad $n$. Sådana polynom finns, således.*
c) *$K$ är isomorf med en kvotkropp $k[X]/(g(x))$ där $g(X)$ är en godtycklig irreducibel faktor i $X^{p^n} - X$, av grad $n$.*
d) *Alla kroppar med $p^n$ element är inbördes isomorfa.*

**.II.3 Sats. Antalssatsen**

*Varje ändlig kropp $K$ har $p^n$ element, $n$ positivt heltal, är spaltningskropp över $k$ till polynomet $X^{p^n} - X$ och består av dess rötter.*

**.II.4 Bevis för antalssatsen.**

$K$ är ett vektorrum över $k$, uppenbarligen av ändlig dimension. Låt $e_1, e_2, \dots e_n$ vara en $k$–bas för $K$. Vi kan uppenbarligen bilda $q = p^n$ olika $k$–lineära kombinationer

$$a_1e_1 + a_2e_2 + \cdots + a_ne_n, \qquad a_1, a_2, \dots, a_n \in k$$

och $K$ har således detta antal element.

Den andra delen av beviset är som för Lilla Fermat. $K^*$ är en grupp med $p^n - 1 = q - 1$ element. Alla nollskilda element $\alpha$ uppfyller alltså $\alpha^{q-1} = 1$. Multiplikation med $\alpha$ ger $\alpha^q = \alpha$ som även satisfieras av nollan. ∎

**.II.5 Bevis för existenssatsen**

Låt $K$ vara spaltningskroppen ifråga. $X^{p^n} - X \in K[X]$ sönderfaller helt i lineära faktorer $X - \theta_i$ där $\theta_i$:na är rötterna i $K$. Vi har tidigare sett att rötterna bildar en kropp, så $K$ måste sammanfalla med denna kropp.

Vi måste nu visa att alla faktorerna är enkla, så att rötternas antal verkligen är lika med gradtalet $p^n$. De flesta böcker brukar använda teorin för formella derivator, men jag använder istället ett snabbt bevis av Israel Herstein.

Låt $\theta \in K$ vara en *godtycklig* rot: $\theta^{p^n} - \theta = 0$ Vi har då

$$X^{p^n} - X = X^{p^n} - \theta^{p^n} - (X - \theta) =$$

$$(X - \theta)^{p^n} - (X - \theta) = (X - \theta)[(X - \theta)^{p^n - 1} - 1]$$

där vi tillämpat Linus Dröm (Freshman's Dream) på den första termen. Faktorn i klammer är $-1$ då $X = \theta$ och är alltså inte delbar med $X - \theta$, som således är en enkel faktor i $X^{p^n} - X$

**.II.6 Bevis för entydighetssatsen**

a) Vi har tidigare visat att mutliplikativa gruppen är cyklisk, $K^* =< \theta >$. Alla nollskilda element är potenser av $\theta$, och nollan är vad den är - samtliga element är alltså polynom i $\theta$

b) Enligt allmänna satser om kroppsutvidgningar är

$$K = k[\theta] \simeq k[X]/(m(X))$$

där $m(X) \in k[X]$ är (det irreducibla) minimalpolynomet för $\theta$. Alla element $\alpha$ i $K$ satisifierar (av tidigare utredda gruppteoretiska skäl)

$$\alpha^{p^n} - \alpha = 0$$

Således är

$$X^{p^n} - X$$

ett dödande polynom för $\theta$ och, enligt den allmänna teorin, delbart med $m(X)$. ∎

En viktig poäng med satsen är att en sådan irreducibel faktor verkligen *finns*

c) Låt $g(X)$ vara en godtycklig irreducibel faktor, av grad $n$, i $X^{p^n} - X$. $K$ består av rötter till $X^{p^n} - X$ så någon av dem, säg $\beta$ är en rot till $g(X)$. Eftersom $g$ är irreducibelt så är $g$ minimalpolynom till $\beta$ och vi har, enligt allmänna satser:

$$k[X]/(g(X)) \simeq k[\beta] \subset K$$

Men ytterleden har samma dimension över $k$ så den sista inklusionen måste vara en likhet, varur den påstådda isomorfin

d) Denna del följer av att alla kroppar $K$ med $p^n$ element har samma beskrivning

∎

I själva verket är alla irreducibla polynom $g(X) \in k[X]$, av grad $n$, faktorer i $X^{p^n} - X$. Se särskilt dokument, som beskriver dess faktorisering.