## .I Universalpolynomet $X^{p^n} - X$

$k$ är kroppen $\mathbf{Z}_p$, av karakteristik $p$. Den allmänna teorin för ändliga kroppar $K$ av karakteristik $p$ kan sammanfattas i följande tre satser (som jag brukar visa på föreläsning)

**.I.1 Sats.** *Spaltningskroppen, över $k$, till polynomet $X^{p^n} - X$, har precis $p^n$ element, och består av dess rötter (dessa är speciellt således olika).*

**.I.2 Sats.** *$K$ har $p^n$ element, $n$ positivt heltal, är spaltningskropp över $k$ till polynomet $X^{p^n} - X$ och består av dess rötter.*

**.I.3 Sats.**

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 $n$.*

Den sista satsens sista del visar att ändliga kroppar med samma antal element är inbördes isomorfa. Beviset använder *inte* den lite abstrakta satsen om spaltningskroppars entydighet.

Ur detta kan vi ge hela sanningen om polynomet $f(X) = X^{p^n} - X$.

**.I.4 Lemma.** *$p$ heltal $\geq 2$, $d, n$ positiva heltal. Då gäller $p^d - 1 | p^n - 1$ om och endast om $d|n$*

**Bevis:** Klart är att $p$ är invertibelt modulo $p^d - 1$, dvs. $(p, p^d - 1) = 1$ och att ordningen av $p$ modulo $p^d - 1$ är exakt $d$. Av teorin för gruppelements ordning följer då att $p^n \equiv 1 \pmod{p^d - 1}$ om och endast om $d|n$. ∎

**.I.5 Sats.** *Alla (moniska) irreducibla faktorer $\in k[X]$ i $f(X)$ är av grad $d|n$*

**Bevis:** Betrakta spaltningskroppen $K$, med $p^n$ element. $K$ består av rötter till $f(X)$ och de är alla olika. Varje rot $\theta$ i $K$ är rot till någon irreducibel faktor $g(X)$ i $f(X)$ och genererar en kropp $E = k[\theta] \subset K$. Om graden av $g$ är $d$ så har kroppen $E$ $p^d$ element. De multiplikativa grupperna $E^*$ och $K^*$ har $p^d - 1$ resp. $p^n - 1$ element. Från gruppteorin vet vi då att $p^d - 1 | p^n - 1$. Av lemmat följer $d|n$ ∎

Observera att vi aldrig använde kroppsgradens multiplikativitet, vilket är ett alternativt bevis.

Vi har alltså visat att $f(X)$ är produkt av irreducibla moniska polynom av grad $d|n$. Vi har nu att visa att *varje* sådant polynom är faktor i $f(X)$ och förekommer exakt en gång. Det senare är dock ingen nyhet; vi vet ju att $f(X)$ har idel enkelrötter i sin spaltningskropp.

Vi visar nu en sats analog med det inledande delbarhetslemmat.

**.I.6 Sats.** *$d|n$ ger $X^{p^d} - X | X^{p^n} - X$*

**Bevis:** Division av båda polynomen med $X$ ger att det räcker att visa $X^e - 1 | X^f - 1$ där $e = p^d - 1 | f = p^n - 1$ enligt lemmat.

Men det är lätt. Med $f = ke$ gäller $X^{ke} - 1 = (X^e - 1)(X^{(k-1)e} + X^{(k-2)e} + \ldots + 1)$. teleskopeffekt, geometrisk summa, osv. ∎

Vi kan nu visa vårt påstående. Om $g(X) \in k[X]$ är irreducibelt av grad $d|n$ så är $k[X]/(g(X))$ en kropp med $p^d$ element, spatlningskropp till $X^{p^d} - X$. För $\theta = \overline{X}$ gäller att $g(X)$ är dess minimalpolynom och $X^{p^d} - X$ ett dödande polynom. Således gäller $g(X) | X^{p^d} - X | X^{p^n} - X$.

Sammanfattningsvis har vi visat:

**.I.7 Sats.** *"Universalpolynomet" $X^{p^n} - X$ är produkten av alla irreducibla moniska polynom i $k[X]$ av grad $d|n$* ∎

En konsekvens är följande. Om vi adjungerar en rot till ett irreducibelt polynom $m(X)$ av grad $n$ så erhåller vi en kropp $K$ med $p^n$ element.

Då sönderfaller detta polynom helt i lineära faktorer över utvidgningskroppen, eftersom multipeln $X^{p^n} - X$ gör det. Och inte bara det. *Alla* irreducibla polynom av grad $d|n$ sönderfaller på detta vis.

Omvänt, om vi adjungerar en rot till ett irreducibelt polynom av grad $d$ blir varje polynom $p(X)$ av grad $n, d|n$ reducibelt över den nya kroppen (med $p^d$ element).

Det sönderfaller i själva verket i faktorer av grad $n/d$. Vi behöver nämligen bara en utvidgning av grad $n/d$, alltså med $p^{n/d}$ element, för att spräcka det.

Fundera på detta.

**.I.8 Exempel:** Vi låter $k = \mathbf{Z}_3$. Vidare låter vi $K$ vara någon kropp med $81 = 3^4$ element. Vi sätter $\Phi_d(X)$ som vi definierar som produkten av alla moniska irrdeucibla polynom i $k[X]$ av grad exakt $= d$. Vi vill bestämma $\Phi_4(X)$

Satsen ovan ger oss genast:

$$\Phi_1 \cdot \Phi_2 \cdot \Phi_4 = X^{3^4} - X = X^{81} - X$$

$$\Phi_1 \cdot \Phi_2 = X^9 - X$$

Så

$$\Phi_4(X) = \frac{X^{81} - X}{X^9 - X} = \frac{X^{80} - X}{X^8 - 1}$$

Detta borde vi kanske känna igen som uttrycket för en geometrisk summa, med kvot $X^8$, första term 1 och $10 = 80/8$ termer. Dvs.

$$\Phi_4(X) = X^{72} + X^{64} + X^{56} + \cdots + X^{16} + X^8 + 1$$

Antalet element av grad 4 är alltså 72; antalet irreducibla moniska polynom av grad 4 är 18.

Sen kan du på samma sätt kontrollera att det finns 6 element av grad 2, och 3 irreducibla polynom av grad 2. De tre element som blir över är förstås de som ligger i grundkroppen.