.I Frobenius.

K är en ändlig kropp, k är dess primkropp. k har p element, där p är ett primtal. K har alltså p^n element där n är vektorrumsdimensionen av K över k.

.I.1 Definition: Frobeniusautomorfismen av K över k är avbildningen

$$\sigma : K \to K$$

given av

$$\sigma(a) = a^p$$

Ordet "automorfism" förklaras längre fram. G. Frobenius (1849-1917) var en tysk matematiker.

Först en grundläggande sats.

.I.2 Sats.

a) σ *är injektiv*
b) σ *är surjektiv*
c) σ *är en homomorfism*
d) $\sigma(a) = a \iff a \in k$, *"k är fixkropp till* σ*"*
e) Avbildningarna $id, \sigma, \sigma^2, \ldots, \sigma^{n-1}, \sigma^n = id, \ldots$ *bildar en cyklisk grupp,* G*, av ordning* n*. Härvid är, i klartext,*

$$\sigma^k(a) = a^{p^k}$$

Bevis:

a) $\sigma(a) = \sigma(b) \iff a^p = b^p \iff a^p - b^p = 0 \iff (a-b)^p = 0 \iff a - b = 0$. Vi har använt Freshman's Dream baklänges.

b) Följer av den just visade injektiviteten, samt att K är ändlig.

c) $(a \pm b)^p = a^p \pm b^p$ enligt Freshman's Dream. $(a \cdot b^{\pm 1})^p = a^p \cdot (b^{\pm 1})^p$ är däremot trivialt.

d) Primkroppen *består av* rötterna till polynomet $X^p - X$ enligt den allmänna teorin.

e) Att $\sigma^n(a) = a$ för alla $a \in K$ följer direkt av att K är spaltningskropp till $X^{p^n} - X$ och består av dess rötter. Så vi har $\sigma^n = \mathrm{id}$.

För att visa att de angivna potenserna bildar en grupp behöver vi bara visa att varje potens har invers; slutenheten under multiplikation (komposition) är klar.

Men av $\sigma^k \cdot \sigma^{n-k} = \sigma^n = \mathrm{id}, 0 \leq k \leq n-1$, följer direkt att de båda angivna potenserna är varandras inverser.

Vi behöver visa att potenserna $\sigma^k, 0 \leq k \leq n-1$ är olika. Om

$$\sigma^j = \sigma^k, 0 \leq j < k \leq n-1$$

följer på vanligt vis (multiplicera båda leden med $(\sigma^{-1})^j$) att $\sigma^{k-j} = \mathrm{id}$. Då skulle ekvationen

$$a^{p^{k-j}} = a$$

gälla för alla $a \in K$. Med $d = k - j$ är emellertid rötterna till $X^{p^d} - X$ enligt den allmänna teorin en delkropp av K med högst $p^d < p^n$ element, och det går ju inte! ∎

Vi har namn på allting. En homomorfism av en kropp (eller ring) till sig själv kallas för en *endomorfism*. Om den samtidigt är bijektiv, alltså en isomorfism, kallas den för en *automorfism*. En sådan uttrycker något slags symmetri i kroppens struktur.

Man kan bevisa att en ändlig kropp inte har andra automorfismer än de n angivna potenserna av Frobenius.

Det enklaste exemplet på en sådan symmetri är komplexkonjugation. I kroppen av komplexa tal betraktar vi avbildningen $\sigma(a + ib) = a - ib$ som ju - som bekant - bevarar summor, skillnader, produkter och kvoter. Dess fixkropp är kroppen av reella tal.

.I.3 Minimalpolynom och Frobenius.

En poäng med att K har n symmetrier över primkroppen är följande. Om ett irreducibelt polynom $m(X) \in k[X]$ har en rot α i K så kan vi skaffa alla dess rötter genom att låta Frobenius verka upprepade gånger på α.

Det är innehållet i följande sats som vi förbereder genom att införa lite beteckningar.

Vi låter $H := \{\sigma^i : \sigma^i(\alpha) = \alpha\}$. H visas vara en delgrupp av G och är alltså själv en cyklisk grupp, $H =< \sigma^e >, 0 \leq e \leq n-1$. H har då $h := |G|/e$ element.

Låt nu $m(X) \in k[X]$ vara minimalpolynomet för α, och d dess grad.

.I.4 Sats.

a)

$$m(X) = (X - \alpha)(X - \sigma(\alpha))(X - \sigma^2(\alpha)) \cdots (X - \sigma^{d-1}(\alpha))$$

med d skilda rötter, samtliga tillhörande K.

b) $\sigma^d(\alpha) = \alpha$

c) $d = e$; graden av $m(X)$ är alltså en faktor i n och kan bestämmas genom upprepad användning av Frobenius.

d) Adjunktion av en enda rot till ett irreducibelt polynom $m(X) \in k[X]$ skapar alltså en kropp E där $m(X)$ sönderfaller helt i lineära faktorer.

Bevis: Beträffande a) är det två saker att visa. Den ena är att elementen

$$\alpha, \sigma(\alpha), \sigma^2(\alpha), \dots \sigma^{d-1}(\alpha)$$

är olika. Den andra är att, om β är en rot till $m(X)$, så är även $\sigma(\beta)$ en rot.

Vi etablerar först vår miljö. α alstrar delkroppen

$$E = k[\alpha] \simeq k(X)/(m(X))$$

av dimension d över k. Den har alltså p^d element. Då vet vi enligt den allmänna teorin att $\alpha^{p^d} = \alpha$, dvs. $\sigma^d(\alpha) = \alpha$, vilket är del b) i satsen.

Om nu $\sigma^j(\alpha) = \sigma^k(\alpha), 0 \leq j < k \leq n-1$ så vi får vi som tidigare $\sigma^{k-j}(\alpha) = \alpha$. Detta visar, på samma sätt som ovan, att α tillhör en delkropp av E med högst $p^{k-j} < p^d$ element. Men det går ju inte, eftersom α *alstrar* hela E. Detta ger det första påståendet.

För det andra påståendet skriver vi ut $m(X)$ med lite termer:

$$m(X) = X^d + a_1 X^{d-1} + a_2 X^{d-2} + \dots + a_d, \quad a_1, a_2, \dots a_d \in k$$

Låt $\beta \in K$ vara en rot:

$$m(\beta) = \beta^d + a_1 \beta^{d-1} + a_2 \beta^{d-2} + \dots + a_d = 0$$

Vi låter nu σ verka på båda leden. Sätt $\beta' := \sigma(\beta)$. Vi utnyttjar att σ är en automorfism som fixerar koefficienterna, eftersom dessa tillhör primkroppen k. Vi får då direkt vårt påstående:

$$m(\beta') = \beta'^d + a_1 \beta'^{d-1} + a_2 \beta'^{d-2} + \dots + a_d = 0$$

Påståendena c) och d) är nu rätt omedelbara; om inte så lämnas de som övning.

∎

.I.5 Exempel: Som ett relativt enkelt exempel bestämmer vi de udda primtal p för vilka kongruensen

$$x^2 \equiv -1 \pmod{p}$$

är lösbar, dvs. de p för vilka polynomet $m(X) = X^2 + 1 \in \mathbf{Z}_p[X]$ är reducibelt.

Vi låter α vara rot till $m(X)$ i någon utvidgningskropp K.

Vi har två fall. Om $\sigma(\alpha) = \alpha$ så ligger α i primkroppen, alltså i $k = \mathbf{Z}_p$. Om däremot $\sigma(\alpha) \neq \alpha$ så måste α tillhöra en större kropp.

I det första fallet har vi

$$\alpha^2 = -1; \quad \alpha^4 = 1; \qquad \alpha^p = \alpha, \quad \alpha^{p-1} = 1$$

Ordningen av α i k^* är 4 och vi måste enligt gruppteorin ha $4|p-1$, dvs. $p \equiv 1 \pmod{4}$.

I det andra fallet har vi

$$\alpha^2 = -1; \quad \alpha^4 = 1; \qquad \alpha^p \neq \alpha, \quad \alpha^{p-1} \neq 1$$

och då måste gälla att $4 \not| p-1$, dvs. $p \not\equiv 1 \pmod 4$, dvs. $p \equiv 3 \pmod 4$.

Dessa båda fall utesluter varandra, så kongruensen $x^2 \equiv -1 \pmod p$ är lösbar, för udda primtal p, om och endast om $p \equiv 1 \pmod 4$.

∎

De vanligaste bevisen för detta bygger på att $\mathbf{Z}_p^*$ är cyklisk. Egentligen har vi inte använt mycket mer än Fermats lilla sats och *existensen* av rotdajunktion.

.I.6 Exempel: Ett litet sidospår. Låt p vara ett primtal $\equiv 1 \pmod 4$. Vi har just sett att det finns ett $r \in \mathbf{Z}$ sådant att $r^2 \equiv -1 \pmod p$, dvs. $p|r^2 - 1$ i $\mathbf{Z}$.

I ringen $\mathbf{Z}[i]$ kan vi skriva $p|(r-i)(r+i)$ och jag påstår att detta medför att p är *reducibelt* som element i denna ring. Ty eljes vore kvotringen $\mathbf{Z}[i]/(p)$ ett integritetsområde (rentav en kropp). Men vi har ju $(r-i+(p))(r+i+(p)) = 0$ i denna ring och varken $r-i+(p)$ eller $r+i+(p)$ är nollklassen, eftersom $p \not| r \pm i$.

p är alltså reducibelt i $\mathbf{Z}[i]$:

$$p = (a+ib)(c+id), \qquad a+ib,\, c+id \neq \pm 1, \pm i$$

För normerna gäller då:

$$p^2 = (a^2+b^2)(c^2+d^2), \qquad a^2+b^2,\, c^2+d^2 \neq 1$$

vilket tvingar

$$p = a^2 + b^2 = c^2 + d^2$$

Varje primtal $p \equiv 1 \pmod 4$ är alltså en summa av två heltalskvadrater.

$p = 2$ är det trivialt och $p \equiv 3 \pmod 4$ är det inte, ty av $a^2 \equiv 0, 1 \quad b^2 \equiv 0, 1 \pmod 4$ följer $a^2 + b^2 \equiv 0, 1, 2 \pmod 4$.

.I.7 Exempel: Man visar lätt att polynomet $m(X) = X^4 + X + 1 \in \mathbf{Z}_2[X]$ är irreducibelt. Det saknar rötter i $\mathbf{Z}_2$ och är inte delbart med det enda irreducibla andragradspolynomet $X^2 + X + 1$.

Det är också lätt att visa att det är primitivt. Låt α = klassen av X, dvs. $X + (X^4 + X + 1)$, i utvidgningskroppen $K = \mathbf{Z}_2[X]/(X^4 + X + 1)$.

Vi kan inte ha $\alpha^3 = 1$ eftersom minimalpolynomets grad är 4. Vi kan inte ha $\alpha^5 = 1$, ty det är lätt att kontrollera att $X^5 - 1 = X^5 + 1$ inte är delbart med $m(X)$. Ordningen av α måste alltså vara den maximala $= 15$.

Alla nollskilda element i K är alltså potenser av α. Vilka av dess potenser har grad två över restkroppen, dvs. vilka satisfierar en irreducibel andragradsekvation?

Vi frågar alltså efter de $\alpha^k, k = 0, 1, 2, \ldots 14$ för vilka $\sigma(\alpha^k) = \alpha^{2k} \neq \alpha^k$ samtidigt som $\sigma^2(\alpha^k) = \alpha^{2^2 k} = \alpha^k$.

Det senare innebär att $4k \equiv k \pmod{15}$, $3k \equiv 0 \pmod{15}$, $k \equiv 0 \pmod{5}$, dvs. $k = 0, 5, 10$ Det första kravet, $\sigma(\alpha^k) = \alpha^{2k} \neq \alpha^k$, utesluter dock $k = 0$ (förstås!). Så vi erhåller potenserna α^5, α^{10}.

Dessa båda måste vara rötter till det enda irreducibla andragradspolynomet, så

$$X^2 + X + 1 = (X - \alpha^5)(X - \alpha^{10})$$

Här är den andra roten lika med Frobenius av den första, dvs. dess kvadrat (och omvänt).

Genom reduktion modulo $X^4 + X + 1$ kan vi naturligtvis skriva α^5, α^{10} som tredjegradspolynom i α.

Vi tittar nu på elementen skilda från α^5, α^{10} samt $0, 1$. Det visar sig att samtliga dessa har grad 4 (vilket kan förklaras med lite fler begrepp ...). Vi vet ju redan att α har grad fyra. Vi får minimalpolynomets övriga rötter genom att utföra Frobenius tre gånger:

$$\alpha, \alpha^2, \alpha^4, \alpha^8, \quad \text{varvid } \alpha^{16} = \alpha.$$

Satsen ovan ger då att

$$m(X) = X^4 + X + 1 = (X - \alpha)(X - \alpha^2)(X - \alpha^4)(X - \alpha^8)$$

En ännu oförbrukad potens är α^7. Upprepad Frobenius ger

$$\alpha^7, \alpha^{14}, \alpha^{28} = \alpha^{13}, \alpha^{26} = \alpha^{11}, \quad \text{varvid } \alpha^{22} = \alpha^7$$

Dessa potenser är inverserna till de ovan funna, t ex är ju $\alpha^7 \cdot \alpha^8 = \alpha^{15} = 1$

Det är lätt att se vi inverterar rötterna till $m(X)$ genom att bilda dess *reciproka* polynom $X^4 m(1/X) = X^4 + X^3 + 1$ - vi vänder helt enkelt koefficienterna bakfram.

Nu hugger vi en av de återstående potenserna, säg α^3, som underkastas samma behandling:

$$\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24} = \alpha^9, \quad \text{obs. att } \alpha^{18} = \alpha^3$$

Här är den första och tredje, resp. den andra och fjärde, potensen, varandras inverser. Minimalpolynomet måste då vara självreciprokt ("palindromiskt"), dvs. oförändrat när vi vänder koefficienterna bakfram. Det kan inte vara

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

ej heller

$$X^4 + X^3 + X + 1 = (X + 1)(X^3 + 1)$$

och absolut inte

$$X^4 + 1 = (X + 1)^4.$$

Det enda som blir över är:

$$X^4 + X^3 + X^2 + X + 1$$

Obs. att α^3 har ordning fem: $(\alpha^3)^5 = \alpha^{15} = 1$ så denna potens är inte primitiv. Det ser vi också genom att multiplicera polynomet ovan med $X + 1 = X - 1$:

$$(X^4 + X^3 + X^2 + X + 1) \cdot (X - 1) = X^5 - 1$$

dvs. alla dess rötter β uppfyller $\beta^5 = 1$.

∎

.I.8 Berlekamp light

Ett annat dokument behandlar Berlekamps faktoriseringsalgoritm, som bygger på Kinesiska Restsatsen och Frobenius

Här ska vi mer ad hoc visa hur Frobenius kan användas till att avgöra om ett polynom är irreducibelt.

Vi låter $f(X) \in k[X]$ vara moniskt, *kvadratfritt*, dvs.

$$f(X) = f_1(X)f_2(X)\cdots f_d(X),$$

där f_d:na är *skilda* moniska irreducibla faktorer. Huruvida ett givet polynom är kvadratfritt kan man avgöra genom att ta reda på sgf med dess formella derivata, via Euklides. Ett polynom är kvadratfritt om och endast om denna sgf är $= 1$.

Vi betraktar nu ringen

$$R = k[X]/(f(X))$$

som är en kropp om och endast om $f(X)$ är irreducibelt. Det viktiga för oss är följande:

1) R innehåller på ett naturligt sätt en isomorf kopia av k, och är således av karakteristik p. Denna kopia består av klasserna av alla konstanta polynom.
2) R är ett vektorrum över k; dess dimension är lika med graden av f.

Vi kan definiera Frobenius för denna ring, som ovan. Precis som ovan gäller att Frobenius fixerar k. Linus' Dröm går fortfarande igenom, så vi har

$$\sigma(a+b) = \sigma(a) + \sigma(b)$$

För $\lambda \in k$ gäller

$$\sigma(\lambda \cdot a) = \sigma(\lambda)\cdot\sigma(a) = \lambda\cdot\sigma(a)$$

eftersom σ fixerar alla element i k. Dvs. Frobenius är *lineär* över k.

Om f är irreducibelt, så att R är en kropp, så har vi tidigare sett att σ fixerar elementen i k, och endast dessa. k–dimensionen av σ:s *fixrum* (dvs. egenrummet till egenvärdet 1) är således $= 1$.

Vi visar nu att sagda fixrum har dimension större än ett, om f är reducibelt. Vi skriver $f(X) = g(X)\cdot h(X)$ där faktorerna är relativt prima, och av positiv grad. Vi löser Bézout:

$$A(X)g(X) + B(X)h(X) = 1$$

För den andra termen i vänsterledet, $e(X) := B(X)h(X)$, gäller att

$$e(X) \equiv 1 \pmod{g(X)}$$

$$e(X) \equiv 0 \pmod{h(X)}$$

Uppenbart gäller också

$$e(X)^p \equiv 1^p \equiv 1 \pmod{g(X)}$$

$$e(X)^p \equiv 0 \pmod{h(X)}$$

Alltså har vi

$$e(X)^p - e(X) \equiv 0 \pmod{g(X)}$$

$$e(X)^p - e(X) \equiv 0 \pmod{h(X)}$$

Eftersom $f(X) = g(X)h(X)$ och faktorerna är relativt prima så ger oss de vanliga delbarhetssatserna att

$$e(X)^p - e(X) \equiv 0 \pmod{f(X)}$$

(möjligen har du bara sett denna delbarhetssats för heltal; men beviset bygger på Bézout och blir därför exakt detsamma för polynom över en kropp).

Klassen av $e(X)$ modulo $f(X)$ fixeras alltså av Frobenius. Det är uppenbart att ingen *konstant* kan satisifiera det första kongruenssystemet. Vi har alltså funnit ett element utanför k, som fixeras av Frobenius. Fixrummet måste alltså ha dimension >1 i detta fall.

M h a Kinesiska Restsatsen bevisas, i det nämnda dokumentet, att dimensionen i själva verket är lika med $d=$ antalet irreducibla faktorer.

.I.9 Sats. *Beteckningar som ovan. $f(X)$ är irreducibelt om och endast om fixrummet till Frobenius har dimension exakt lika med ett.*

.I.10 Exempel: Vi låter p vara udda, och $f(X) = X^4 + 1$, med formell derivata $4X^3$. Upenbarligen saknar dessa båda polynom gemensamma faktorer, så $f(X)$ är kvadratfritt.

Låt oss undersöka fallet $p \equiv 3 \pmod{8}$.

En bas för R består av klasserna $1, x, x^2, x^3$. Vi låter alltså små bokstäver beteckna restklasser. Här är således $x^4 = -1, \quad x^8 = 1$.

Vi låter Frobenius verka på dessa, vilket ger oss $1, x^p, x^{2p}, x^{3p}$. Här ska vi nu reducera exponenterna modulo 8 så basbilderna är $1, x^3, x^6 = -x^2, x^9 = x$.

Basbildernas koordinater ställs upp som kolonner i en avbildningsmatris:

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

Egenvektorerna till egenvärdet 1 får vi genom att lösa ett homogent ekvationssystem, där vi subtraherat 1 från diagonalelementet:

$$\left(\begin{array}{cccc|c} 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 1 & 0 \\ 0 & 0 & -2 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 \end{array}\right)$$

Här kan vi utan vidare stryka den första och den sista ekvationen (eftersom den senare säger samma sak som den andra). Alltså ser vi utan plåga att systemet har 2-parametrig lösning, dvs. $X^4 + 1$ är reducibelt (med två irreducibla faktorer).

Du inviteras att undersöka p ur de övriga tre klasserna modulo 8, speciellt $p \equiv 7 \pmod 8$