

3. Cirkedelingspolynomier. Endelige legemer.

(3.1) Definition. Lad n være et naturligt tal. Et element ζ i et legeme L kaldes en n 'te *enhedsrod*, hvis $\zeta^n = 1$ (hvor 1 er et-elementet i L). Ækvivalent er ζ altså en n 'te enhedsrod, hvis ζ er rod i polynomiet $X^n - 1$. Ligningen $\zeta^n = 1$ medfører øjensynlig, at $\zeta \neq 0$, og at ζ i legemets multiplikative gruppe L^* har en orden, der er divisor i n . Hvis ζ har orden n , dvs hvis $\zeta^n = 1$ og $\zeta^j \neq 1$ for $1 \leq j < n$, kaldes ζ en *primitiv* n 'te enhedsrod.

Hvis legemet er de komplekse tals legeme $\mathbb{C}$, har polynomiet $X^n - 1$ netop n rødder. Det er velkendt, at de komplekse n 'te enhedsrødder er tallene af formen,

$$\zeta = e^{2\pi i a/n}, \quad \text{hvor } 0 \leq a < n.$$

Sættes $\zeta_n := \exp 2\pi i/n$, er det altså tallene af formen $\zeta = \zeta_n^a$, altså potenserne af tallet ζ_n . De komplekse n 'te enhedsrødder udgør derfor den cykliske gruppe frembragt af den specielle enhedsrod ζ_n . Øjensynlig har ζ_n orden n . Heraf følger, at ζ_n^a har orden lig med $n/(a, n)$. Specielt ses, at ζ_n^a har orden n , hvis og kun hvis a er primisk med n . Antallet af primitive komplekse n 'te enhedsrødder er altså $\varphi(n)$, hvor φ er Euler's φ -funktion. I legemet $\mathbb{R}$ er de eneste enhedsrødder naturligvis 1 og -1 (af ordener 1 og 2).

(3.2) Definition. Polynomiet,

$$\Phi_n := \prod_{\zeta} (X - \zeta),$$

hvor ζ gennemløber de $\varphi(n)$ primitive, komplekse n 'te enhedsrødder, kaldes det n 'te *cirkedelingspolynomium*. Polynomiet Φ_n er øjensynligt et normeret polynomium af grad $\varphi(n)$.

(3.3) Sætning. Cirkedelingspolynomierne Φ_n tilfredsstiller ligningerne,

$$X^n - 1 = \prod_{d|n} \Phi_d, \tag{3.3.1}$$

hvor produktet på højresiden er over alle positive divisorer d i n .

Bevis. Polynomiet på venstresiden af ligningen kan faktoreriseres:

$$X^n - 1 = \prod_{\xi} (X - \xi),$$

hvor ξ gennemløber de n komplekse rødder i polynomiet, dvs de n 'te enhedsrødder. Grupperes i produktet faktorerne $X - \xi$ svarende til at ξ har en bestemt orden d (nødvendigtvis med $d|n$), fremkommer polynomiet Φ_d . Heraf fås den ønskede formel. $\square$

Korollar. Cirkedelingspolynomiet Φ_n har koefficienter i $\mathbb{Z}$.

Bevis. Formlen i Sætningen kan skrives:

$$X^n - 1 = \Phi_n \Pi_n, \quad \text{hvor } \Pi_n = \prod_{d|n, d < n} \Phi_d.$$

Heraf ses, at Φ_n fremkommer som kvotient, når polynomiet $X^n - 1$ divideres med polynomiet Π_n . Polynomiet Π_n er øjensynlig normeret. Idet Korollarets påstand vises ved fuldstændig induktion efter n , kan det antages, at Π_n har hele koefficienter. Heraf følger, at kvotienten Φ_n også har hele koefficienter. $\square$

(3.4) Eksempel. Øjensynlig er

$$\begin{aligned}\Phi_1 &= X - 1, & \Phi_2 &= X + 1, & \Phi_4 &= X^2 + 1, \\ \Phi_3 &= X^2 + X + 1 & \text{og} & & \Phi_6 &= X^2 - X + 1.\end{aligned}$$

Ifølge Sætning (3.3), jfr. beviset for Korollaret, fremkommer Φ_n ved at dividere polynomiet $X^n - 1$ med produktet af førstegradspolynomierne $X - \xi$, hvor ξ er en n 'te enhedsrod af orden strengt mindre end n . Hvis $n = p^r$ er en primtalspotens, så har en n 'te enhedsrod ξ orden strengt mindre end n , netop når $\xi^{p^{r-1}} = 1$. Følgelig er

$$\Phi_{p^r} = \frac{X^{p^r} - 1}{X^{p^{r-1}} - 1} = X^{p^{r-1}(p-1)} + X^{p^{r-1}(p-2)} + \dots + X^{p^{r-1}} + 1.$$

Specielt fås for et primtal p , at

$$\Phi_p = X^{p-1} + X^{p-2} + \dots + X + 1,$$

og for potenser af 2:

$$\Phi_{2^r} = X^{2^{r-1}} + 1.$$

Betragt $n = 48$. Hvis $\xi^{48} = 1$, og ξ ikke har orden 48, så har ξ orden d , hvor d er en ægte divisor i 48. Enten er altså d divisor i 24, eller $d = 16$. Følgelig er

$$\Phi_{48} = \frac{X^{48} - 1}{(X^{24} - 1)\Phi_{16}} = \frac{X^{24} + 1}{X^8 + 1} = X^{16} - X^8 + 1.$$

(3.5) Karakteristik. Betragt et vilkårligt legeme L . Den kanoniske ringhomomorfi $\mathbb{Z} \rightarrow L$ er som bekendt afbildningen $k \mapsto k1$, der afbilder k på den k 'te (additive) potens af et-elementet 1 i L . For $k \in \mathbb{N}$ er altså

$$k1 = \overbrace{1 + \dots + 1}^k.$$

Kernen er et ideal i $\mathbb{Z}$, altså af formen $\mathbb{Z}p$, hvor $p \geq 0$. Tallet p kaldes som bekendt *karakteristikken* af L . Karakteristikken kan være 0, svarende til at homomorfien $\mathbb{Z} \rightarrow L$ er injektiv; i dette tilfælde kan vi opfatte $\mathbb{Z}$ som en delring af L ,

$$\mathbb{Z} \hookrightarrow L.$$

Hvis karakteristikken af et legeme ikke er 0, må den som bekendt være et primtal. I dette tilfælde giver Isomorfisætningen for ringe en naturlig isomorfi mellem kvotienten $\mathbb{Z}/p$ og billedringen. Vi kan altså opfatte legemet $\mathbb{F}_p = \mathbb{Z}/p$ (med p elementer) som delring af L ,

$$\mathbb{F}_p \hookrightarrow L.$$

Karakteristik kan som bekendt defineres for en vilkårlig kommutativ ring R . I primtals-karakteristik gælder følgende nyttige resultat:

Freshman's Dream. Når karakteristikken af R er et primtal p , så er, for alle $x, y \in R$,

$$(x + y)^p = x^p + y^p, (xy)^p = x^p y^p, 1^p = 1. \quad (3.5.1)$$

De to sidste ligninger er blot almindelige potensregler, den første følger ved at anvende binomialformlen: da p er et primtal, er binomialkoefficienterne $\binom{p}{i}$ for $0 < i < p$ delelige med p , og leddene $\binom{p}{i} x^i y^{p-i}$ er derfor 0 i R .

Et polynomium f i $\mathbb{Z}[X]$ giver via den kanoniske homomorfi et polynomium i $L[X]$. I karakteristik 0 fremkommer det via inklusionen $\mathbb{Z}[X] \hookrightarrow L[X]$. I positiv karakteristik p reduceres først koefficienterne i f modulo p ; det reducerede polynomium ligger så i delringen $\mathbb{F}_p[X] \subseteq L[X]$. Det fører sædvanligvis ikke til misforståelser, hvis det reducerede polynomium også betegnes med f . I alle tilfælde kan vi, for et element $\xi \in L$, indsætte ξ i f , og specielt undersøge, om ξ er rod i f .

(3.6) Sætning. Lad p være karakteristikken af legemet L . Da gælder, for $\zeta \in L$ og $n \in \mathbb{N}$, at ζ har orden n i L^* , hvis og kun hvis $\Phi_n(\zeta) = 0$ og p ikke går op i n .

Bevis. Den sidste betingelse, $p \nmid n$, er naturligvis altid opfyldt, hvis $p = 0$. Hvis p er et primtal, og n er ordenen af et element ζ i L , er den også opfyldt. Antag nemlig, indirekte, at ζ har orden n , hvor $n = dp$. Da er

$$0 = \zeta^n - 1 = \zeta^{dp} - 1 = (\zeta^d - 1)^p,$$

hvor den sidste ligning følger af (3.5.1). Følgelig er også $\zeta^d = 1$, i modstrid med at ordenen n er den mindste positive eksponent med $\zeta^n = 1$.

Vi kan altså, i resten af beviset, antage, at $p \nmid n$. Af (3.3.1) får vi, eventuelt ved at reducere koefficienterne, følgende ligning i $L[X]$:

$$X^n - 1 = \prod_{d \mid n} \Phi_d. \quad (3.6.1)$$

Af (3.6.1) følger umiddelbart, at hvis ζ er rod i Φ_n , så er ζ rod i $X^n - 1$, altså $\zeta^n = 1$, og omvendt, hvis $\zeta^n = 1$, så er ζ rod i et af polynomierne Φ_d for $d \mid n$.

Antag, at ζ har orden n . Da er $\zeta^n = 1$, og ζ er dermed rod i et polynomium Φ_d for $d \mid n$. Specielt er også $\zeta^d = 1$. Da ζ har orden n , er det udelukket, at $d < n$. Altså er ζ rod i Φ_n .

Antag omvendt, at ζ er rod i Φ_n . Da er $\zeta^n = 1$, så ζ 's orden er en divisor e i n . Da $\zeta^e = 1$ fås, ved at betragte (3.6.1) for $n := e$, at ζ må være rod i et Φ_d , hvor $d \mid e$. Antag, indirekte, at $e < n$. Da er $d < n$, og ζ er altså rod i to forskellige faktorer på højresiden af (3.6.1). Vi får derfor en ligning $X^n - 1 = (X - \zeta)^2 g$ med et polynomium $g \in L[X]$. Ved differentiation fås ligningen,

$$nX^{n-1} = (X - \zeta)(2g + (X - \zeta)g').$$

Ved indsættelse af ζ fås $n\zeta^{n-1} = 0$, og videre, ved multiplikation med ζ , fås $n1 = 0$, i modstrid med at karakteristikken p ikke var divisor i n . $\square$

(3.7) Bemærkning. Hvis G er en endelig undergruppe af den multiplikative gruppe L^* , så er G cyklisk. Dette er velkendt (og vi brugte det i (2.2), hvor vi udnyttede, at den multiplikative gruppe $\mathbb{F}_p^*$ er cyklisk). Alternativt kan vi udnytte Sætningen ovenfor.

Lad n være ordenen af G . Da er $\xi^n = 1$ for alle elementer $\xi \in G$. Polynomiet $X^n - 1$ er normeret af grad n , og det har n forskellige rødder i L , nemlig de n elementer $\xi_1, \dots, \xi_n$ i G . Altså gælder i $L[X]$ ligningen,

$$X^n - 1 = (X - \xi_1) \cdots (X - \xi_n). \quad (3.7.1)$$

Det skal vises, at et af elementerne ξ_i i G har orden n . Hertil bruges Sætningen.

Ved differentiation og indsættelse af ξ_1 i (3.7.1) fås ligningen,

$$n\xi_1^{n-1} = (\xi_1 - \xi_2) \cdots (\xi_1 - \xi_n).$$

Højresiden er forskellig fra 0. Altså kan n , som indgår i venstresiden, ikke være delelig med karakteristikkens af L .

Af (3.7.1) og (3.6.1) slutes, at hver faktor Φ_d på højresiden af (3.6.1) må være et produkt af visse af førstegradsfaktorerne $X - \xi_j$ (lige så mange som graden af Φ_d). Specielt må Φ_n være et sådant produkt, og heraf fremgår videre, at Φ_n har en rod ξ_i blandt elementerne ξ_j . Ifølge Sætningen har ξ_i orden n . Den cykliske undergruppe frembragt af ξ_i har altså orden n , og ξ_i må derfor være en frembringer for G . Altså er G cyklisk.

(3.8) Sætning. *Lad p være et primtal, primisk med n . Betragt i $\mathbb{F}_p[X]$ cirkeldelingspolynomiet $\Phi_n(X)$, og i Φ_n en irreducibel divisor $f \in \mathbb{F}_p[X]$ af grad r . Da er kvotientringen $K := \mathbb{F}_p[X]/(f)$ et legeme med p^r elementer, som omfatter $\mathbb{F}_p$, og restklassen $\xi := (X \bmod f)$ er en primitiv n 'te enhedsrod i K . Yderligere er r lig med ordenen af restklassen $[p]_n$ i $(\mathbb{Z}/n)^*$.*

Bevis. Det er en velkendt beskrivelse af en polynomiumskvotient $K := \mathbb{F}_p[X]/(f)$, at når f har grad r , så er $\mathbb{F}_p \subseteq K$ og elementerne i K kan entydigt skrives

$$\alpha = a_0 + a_1\xi + \cdots + a_{r-1}\xi^{r-1} \quad (3.8.1)$$

med $a_i \in \mathbb{F}_p$. Der er p muligheder for a_i , og altså p^r muligheder for α . Derfor er $|K| = p^r$. Yderligere er det velkendt, når f er irreducibel, at hovedidealet (f) er et maksimalideal, og at kvotienten $K := \mathbb{F}_p[X]/(f)$ derfor er et legeme.

Homomorfien $\mathbb{F}_p[X] \rightarrow \mathbb{F}_p[X]/(f)$ er bestemt ved $F(X) \mapsto F(\xi)$. Specielt er $f(\xi) = 0$, og $\Phi_n(\xi) = 0$, fordi f er divisor i Φ_n . Af Sætning (3.6) fremgår, at ξ har orden n i K^* .

Den multiplikative gruppe K^* har orden $p^r - 1$. Derfor er ordenen n divisor i $p^r - 1$. Med andre ord er $p^r \equiv 1 \pmod{n}$, eller $[p]_n^r = 1$ i $(\mathbb{Z}/n)^*$. Restklassen $[p]_n$ i $(\mathbb{Z}/n)^*$ har altså en orden, som er divisor i r . Det påstås, at ordenen må være lig med r . Antag hertil for et naturligt tal s , at $[p]_n^s = 1$ i $(\mathbb{Z}/n)^*$; det skal vises, at $s \geq r$. Af antagelsen følger, at n er divisor i $p^s - 1$, og derfor er $\xi^{p^s-1} = 1$. Følgelig er $\xi^{p^s} = \xi$. Heraf følger videre, at $(\xi^i)^{p^s} = \xi^i$. Af Fermat's lille sætning følger, for $a \in \mathbb{F}_p$, at $a^p = a$, og så er også $a^{p^s} = a$. Af Freshman's Dream følger så, at højresiden i (3.8.1) ikke ændres, når den opløftes til potensen p^s . Derfor er $\alpha^{p^s} = \alpha$ for alle $\alpha \in K$. Polynomiet $X^{p^s} - X$ har derfor de p^r elementer i K som rødder. Da graden mindst er antallet af rødder, følger det, at $p^s \geq p^r$. Altså er $s \geq r$, som ønsket. $\square$

(3.9) Korollar. For hver primtalspotens $q = p^r$ findes et legeme K med q elementer, fx bestemt som kvotienten,

$$K := \mathbb{F}_p[X]/(f),$$

hvor f i $\mathbb{F}_p[X]$ er en irreducibel divisor i Φ_{q-1} . I denne beskrivelse er sideklassen $\xi := (X \bmod f)$ en frembringer for den cykliske gruppe K^* . Yderligere gælder, at alle legemer med q elementer er isomorfe med K . Mere generelt gælder, at hvis L er et legeme med p^s elementer, så findes en homomorfi $K \hookrightarrow L$, hvis og kun hvis $r \mid s$.

Bevis. Med $n := p^r - 1$ er det klart, at restklassen af p modulo n har orden r i $(\mathbb{Z}/n)^*$. Derfor kan (3.8) anvendes. Det følger, at f har grad r . Derfor er $|K| = p^r$. Yderligere har ξ orden $n = p^r - 1$, og da $|K^*| = p^r - 1$, må ξ være en frembringer for gruppen K^* .

Lad nu L være et legeme med p^s elementer. Antag først, at der findes en homomorfi $K \rightarrow L$. En homomorfi mellem legemer er som bekendt altid injektiv (antyd det med skrivemåden $K \hookrightarrow L$), så vi kan opfatte K som dellegeme af L . Specielt kan L opfattes som vektorrum over K , idet multiplikation af en vektor $u \in L$ med en skalar $\alpha \in K$ blot er produktet αu i legemet L . Hvis d er dimensionen af L som vektorrum over K , kan elementerne i L , efter valg af basis, beskrives ved koordinatsæt med d koordinater fra K . Derfor er $|L| = |K|^d$, altså $p^s = (p^r)^d$. Derfor er $r \mid s$.

Antag omvendt, at $r \mid s$. Så er $n = p^r - 1$ divisor i $p^s - 1$. Da L^* har orden $p^s - 1$, er alle $p^s - 1$ elementer i L^* rødder i polynomiet $X^{p^s-1} - 1 \in L[X]$. Polynomiet $X^{p^s-1} - 1$ er derfor lig med produktet af de $p^s - 1$ faktorer $X - \alpha$ svarende til elementerne $\alpha \in L^*$. På den anden side er f divisor i Φ_n , som er divisor i $X^n - 1$, som er divisor i $X^{p^s-1} - 1$. Derfor må f (efter normering) være lig med produktet af r af faktorerne $X - \alpha$. Specielt har f altså en rod i L . Betragt nu ringhomomorfien,

$$\mathbb{F}_p[X] \rightarrow L \quad \text{bestemt ved } F(X) \mapsto F(\alpha).$$

Da $f(\alpha) = 0$, ligger f i kernen, og derfor er hovedidealet (f) indeholdt i kernen. Kernen er et ægte ideal, og da hovedidealet er et maksimalideal, må ringhomomorfien kerne være lig med hovedidealet (f) . Isomorfiætningen giver nu en isomorfi af $K = \mathbb{F}_p[X]/(f)$ på billedringen, og dermed den ønskede homomorfi $K \hookrightarrow L$.

I specialtilfældet, hvor $s = r$, dvs hvor L er et legeme med q elementer, må denne injektive homomorfi være en isomorfi. Alle legemer med q elementer er altså isomorfe med K . $\square$

(3.10) Korollar. Lad p være et primtal. For primopløsningen af $X^{p^k} - X$ (for $k \geq 1$) i $\mathbb{F}_p[X]$ gælder da, at primfaktorerne er samtlige (normerede) irreducible polynomier i $\mathbb{F}_p[X]$ af en grad, som går op i k , og hver af faktorerne forekommer præcis én gang.

Bevis. Hvis en primfaktor g indgik to gange, ville vi have en ligning $X^{p^k} - X = g^2 h$ i $\mathbb{F}_p[X]$, og ved differentiation ville vi få:

$$-1 = g(2g'h + gh'),$$

hvilket er en modstrid, da g ikke kan være konstant.

30. september 2009

Lad f være et normeret, irreducibelt polynomium i $\mathbb{F}_p[X]$, og lad r betegne graden af f . Det skal vises, at

$$f \mid X^{p^k} - X \iff r \mid k.$$

Betragt hertil kvotienten $K := \mathbb{F}_p[X]/(f)$ og ækvivalensklassen $\xi := (X \bmod f)$. Da er K et legeme med p^r elementer og ξ er rod i f . Hvis $\xi \neq 0$, så ligger ξ i gruppen K^* , der har orden $p^r - 1$, og så er $\xi^{p^r-1} = 1$; specielt er $\xi^{p^r} - \xi = 0$. Den sidste ligning gælder trivielt, hvis $\xi = 0$. Polynomiet $X^{p^r} - X$ afbildes altså i 0 ved homomorfien $F(X) \mapsto F(\xi)$; det ligger altså i hovedidealet (f) . Derfor er f divisor i $X^{p^r} - X$.

Antag først, at $r \mid k$. Da er $p^r - 1 \mid p^k - 1$. Følgelig er $X^{p^r-1} - 1 \mid X^{p^k-1} - 1$, og ved multiplikation med X fås $X^{p^r} - X \mid X^{p^k} - X$. Da vi har set, at $f \mid X^{p^r} - X$, følger det, at $f \mid X^{p^k} - X$.

Antag omvendt, at $f \mid X^{p^k} - X$, altså at $\xi^{p^k} - \xi = 0$. Det skal vises, at $r \mid k$. Det er klart, hvis $r = 1$, så vi kan antage, at $r > 1$. Specielt er så $f \neq X$, og derfor er $\xi \neq 0$. Da $\xi^{p^k} = \xi$, følger det, at $\xi^{p^k-1} = 1$. Lad n være ordenen af ξ . Så er $\Phi_n(\xi) = 0$, og derfor er f divisor i Φ_n . Af Sætning (3.8) følger så, at r er ordenen af restklassen $[p]_n$ i $(\mathbb{Z}/n)^*$. På den anden side er n divisor i $p^k - 1$. Men så er $p^k \equiv 1 \pmod{n}$, og derfor er k et multiplum af ordenen af $[p]_n$, dvs et multiplum af r , som ønsket. $\square$

(3.11) Eksempel. For at konstruere et legeme $\mathbb{F}_{16}$ med $2^4 = 16$ elementer, og heri en frembringer for gruppen $\mathbb{F}_{16}^*$, betragtes cirkeldelingspolynomiet Φ_{15} . Man finder:

$$\Phi_{15} = \frac{X^{15} - 1}{(X^5 - 1)(X^2 + X + 1)} = \frac{X^{10} + X^5 + 1}{X^2 + X + 1} = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1.$$

Korollar (3.9) forudsiger, at dette polynomium modulo 2, dvs i $\mathbb{F}_2[X]$, er et produkt af irreducible polynomier af grad 4. Det er let at se, at der modulo 2 gælder:

$$X^8 + X^7 + X^5 + X^4 + X^3 + X + 1 = (X^4 + X^3 + 1)(X^4 + X + 1).$$

De to polynomier på højresiden er altså irreducible i $\mathbb{F}_2[X]$. Det søgte legeme kan altså fx beskrives som $\mathbb{F}_{16} := \mathbb{F}_2[X]/(X^4 + X + 1)$. Ved denne beskrivelse er restklassen ξ , af X modulo $(X^4 + X + 1)$, en frembringer for den multiplikative gruppe $\mathbb{F}_{16}^*$.

Bemærk, hvordan man regner i det således konstruerede legeme $\mathbb{F}_{16}$: Elementerne har formen

$$r = r_0 + r_1\xi + r_2\xi^2 + r_3\xi^3,$$

og de svarer til 4-sæt (r_0, r_1, r_2, r_3) af restklasser modulo 2. Addition af 4-sæt er blot koordinatvis addition. Multiplikation er bestemt ved ligningen,

$$\xi^4 = \xi + 1;$$

heraf følger fx, at $\xi^5 = \xi + \xi^2$, at $\xi^6 = \xi^2 + \xi^3$, at $\xi^7 = \xi^3 + \xi^4 = \xi^3 + \xi + 1$, osv.

Det skal understreges, at det i almindelighed er en ikke-triviell opgave at faktorisere cirkeldelingspolynomierne modulo p . I det simpleste tilfælde, $r = 1$ (altså $q = p$), af (3.9), vides, at de irreducible divisorer i Φ_{p-1} er førstegradsfaktorer. Det er førstegradsfaktorerne $X - a$, hvor restklassen a er *primitiv rod modulo p* , dvs en frembringer for den cykliske gruppe $\mathbb{F}_p^*$, og det er ikke-trivielt at bestemme primitive rødder modulo p (når $p \gg 0$).

(3.12) Eksempel. Betragt $q = 49$, hvor altså $p = 7$. Vi har

$$\Phi_{48} = X^{16} - X^8 + 1.$$

Sætningen forudsiger, at dette polynomium modulo 7 er et produkt af (nødvendigvis 8) andengradspolynomier.

Et legeme med 49 elementer kan naturligvis konstrueres som en kvotient $\mathbb{F}_7[X]/(g)$ for et vilkårligt irreducibelt andengradspolynomium g . Fx er $g = X^2 + 1$ et sådant polynomium, idet polynomiet modulo 7 øjensynlig ikke har rødder. Lad i betegne restklassen af X i kvotientringen $L := \mathbb{F}_7[X]/(X^2 + 1)$. Da har elementerne i L formen $a + ib$, hvor $a, b \in \mathbb{F}_7$; regning foregår ved at udnytte, at $i^2 = -1$. Specielt har i orden 4. For at bestemme et element $a + ib$ af orden 8, løses ligningen $(a + ib)^2 = i$, altså

$$a^2 - b^2 = 0, \quad 2ab = 1;$$

en løsning er $(a, b) = (2, 2)$, så $2 + 2i$ har orden 8. Et element af orden 16 bestemmes ved at løse $(c + id)^2 = 2 + 2i$, altså

$$c^2 - d^2 = 2, \quad 2cd = 2.$$

En løsning er $(c, d) = (5, 3)$. Elementet $5 + 3i$ har altså orden 16. Endelig, da 2 øjensynlig har orden 3, følger det, at $2(5 + 3i) = 3 - i$ har orden 48. Dette element er den ene rod i

$$f = X^2 - 6X - 4 = X^2 + X - 4.$$

Vi kan altså også opfatte L som kvotienten $\mathbb{F}_{49} := \mathbb{F}_7[X]/(X^2 + X - 4)$: elementerne har formen $a + b\xi$, med $a, b \in \mathbb{F}_7$, og regning i $\mathbb{F}_{49}$ er bestemt ved $\xi^2 = 4 - \xi$. Elementet ξ har orden 48.

(3.13) Korollar. Lad $\alpha_p(r)$ betegne antallet af irreducible normerede polynomier af grad r i $\mathbb{F}_p[X]$. Da er $p^r = \sum_{d|r} d\alpha_p(d)$, og følgelig er

$$\alpha_p(r) = \frac{1}{r} \sum_{d|r} p^{r/d} \mu(d),$$

hvor μ er Möbius-funktionen.

Bevis. Produktet af samtlige irreducible polynomier af grad $d|r$ er ifølge Korollar (3.10) lig med $X^{p^r} - X$. Den første anførte ligning følger nu ved sammenligne graderne, og heraf følger den anden ligning ved Möbius-inversion. $\square$

(3.14) Bemærkning. Af (3.8) fremgår, hvordan man undersøger, om polynomiet $\bar{\Phi}_n$ (fremkommet ved at reducere koefficienterne i Φ_n modulo p) er irreducibelt i $\mathbb{F}_p[X]$, hvor $p \nmid n$. Det fremgår mere præcist, hvordan man bestemmer graden af de irreducible faktorer f , der indgår i primopløsningen af $\bar{\Phi}_n \in \mathbb{F}_p[X]$.

I primopløsningen af $\bar{\Phi}_n$ i $\mathbb{F}_p[X]$ som produkt af irreducible, normerede polynomier er faktorerne i øvrigt indbyrdes forskellige. Antag nemlig indirekte, for et irreducibelt polynomium $f \in \mathbb{F}_p[X]$, at f^2 er divisor i $\bar{\Phi}_n$. Konstruktionen i Sætning (3.8) giver et legeme $K \supseteq \mathbb{F}_p$, hvori f har en rod ξ . Da f^2 er divisor i $\bar{\Phi}_n$, er ξ dobbeltrod i $\bar{\Phi}_n$. Men det er i modstrid med, at ξ er en primitiv n 'te enhedsrod, hvorfor polynomiet $\bar{\Phi}_n$ i K har $\varphi(n)$ forskellige rødder, nemlig potenserne ξ^a med $(a, n) = 1$.

Det er et fundamentalt resultat i algebraisk talteori, at Φ_n altid er irreducibelt i $\mathbb{Q}[X]$.

Betragt hertil i $\mathbb{Q}[X]$ en normeret, irreducibel divisor F i Φ_n . Det skal vises, at $F = \Phi_n$. Da $F \mid \Phi_n$, er enhver (kompleks) rod i F også rod i Φ_n , altså en primitiv n 'te enhedsrod. Det skal altså omvendt vises, at enhver primitiv n 'te enhedsrod er rod i F . Ud fra en given primitiv n 'te enhedsrod ζ fås de øvrige som potenserne ζ^a , med $a \geq 1$ primisk med n . Eksponenten a kan skrives som produkt af primtal p med $p \nmid n$. Det er derfor nok at vise følgende påstand:

Hvis ζ er rod i F og p er et primtal med $p \nmid n$, så er ζ^p også rod i F .

I beviset for påstanden bruges, at ethvert polynomium i $\mathbb{Q}[X]$ med ζ som rod er et multiplum af F . Det følger af at polynomiumsringen $\mathbb{Q}[X]$ er et hovedidealområde: Polynomierne i $\mathbb{Q}[X]$ med ζ som rod er et ideal; derfor findes et normeret polynomium F_0 således, at dette ideal består af samtlige multipla af F_0 . Da $F(\zeta) = 0$, er F et multiplum af F_0 ; da F er irreducibel, og altså kun har trivielle divisorer, er $F = F_0$. Idealet består derfor af alle multipla af F .

Antag nu, indirekte, at ζ^p ikke er rod i F . Polynomiet $\Phi_n \in \mathbb{Q}[X]$ er et produkt af irreducible, normerede faktorer, og en af dem er F . Da ζ^p er rod i Φ_n , må ζ^p så være rod i en af de andre irreducible faktorer; lad os kalde den G . Fra primopløsningen i $\mathbb{Q}[X]$ af $\Phi_n(X)$ får vi så specielt en faktorisering i $\mathbb{Q}[X]$:

$$\Phi_n = FGH. \quad (*)$$

Da polynomierne er normerede og venstresiden har hele koefficienter, følger det af et korollar til Gauss's Lemma, at F, G, H har koefficienter i $\mathbb{Z}$. Da ζ^p er rod i G , er ζ rod i polynomiet $G(X^p)$. Altså er $G(X^p)$ et multiplum af F . Derfor findes en faktorisering $G(X^p) = QF$. At Q har koefficienter i $\mathbb{Z}$ følger fx af Sætningen om division med rest.

Nu reduceres koefficienterne modulo p . Af (*) fås $\bar{\Phi}_n = \bar{F}\bar{G}\bar{H}$. Videre er koefficienterne i $\bar{G}$ elementer i $\mathbb{F}_p$, og for $a \in \mathbb{F}_p$ gælder $a^p = a$ ifølge Fermat's lille sætning. Derfor følger det af Freshman's Dream, at $(\bar{G}(X))^p = \bar{G}(X^p)$. Af $QF = G(X^p)$ følger derfor, at $\bar{F}\bar{Q} = \bar{G}^p$. Vi har altså følgende faktoriseringer i $\mathbb{F}_p[X]$:

$$\bar{\Phi}_n = \bar{F}\bar{G}\bar{H}, \quad \bar{Q}\bar{F} = \bar{G}^p. \quad (**)$$

Betragt nu i $\mathbb{F}_p[X]$ en irreducibel, normeret divisor f i $\bar{F}$. Af den anden faktorisering følger, at f er divisor i $\bar{G}^p$, og heraf følger, da f er irreducibel, at f er divisor i $\bar{G}$. I den første faktorisering er f altså divisor i både $\bar{F}$ og $\bar{G}$, og derfor er f^2 divisor i $\bar{\Phi}_n$. Men det er en modstrid, idet primdivisorerne i primopløsningen af $\bar{\Phi}_n$ som nævnt er indbyrdes forskellige.

Hermed er påstanden ovenfor bevist, og det er godtgjort, at Φ_n er irreducibelt i $\mathbb{Q}[X]$.

(3.15) Bemærkning. Cirkeldelingspolynomier har mange anvendelser. Lad os her vise, for et naturligt tal $n > 1$, at der er uendelig mange primtal p med $p \equiv 1 \pmod{n}$. Lad der være givet k primtal $p_1, \dots, p_k$. Vi viser, at der eksisterer et primtal p , forskelligt fra de givne, med $p \equiv 1 \pmod{n}$.

Vi bemærker først, at for hvert naturligt tal h er værdien $\Phi_n(h)$ et helt tal (fordi Φ_n har hele koefficienter), og når $h \geq 2$ er $\Phi_n(h) > 1$. Mere præcist gælder uligheden,

$$(h-1)^{\varphi(n)} < \Phi_n(h), \text{ når } h \geq 1. \quad (3.15.1)$$

Tallet $\Phi_n(h)$ er nemlig produktet af faktorerne $h - \xi$ for primitive n 'te enhedsrødder ξ . For hver sådan er også $\bar{\xi} = \xi^{-1}$ en primitiv n 'te enhedsrod. Idet (3.15.1) er trivielt for $n = 2$, antager vi $n > 2$, og så er $\bar{\xi} \neq \xi$. Med $h - \xi$ forekommer altså også $h - \bar{\xi}$ som faktor, og produktet af disse to faktorer er positivt. Altså er $\Phi_n(h)$ positiv (endda for *alle* reelle tal h , når $n > 2$).

Numerisk er $|h - \xi|$ lig med afstanden fra h til ξ . Da ξ ligger på enhedscirklen, og $\xi \neq 1$, er $|h - \xi| > |h - 1|$. Altså gælder (3.15.1).

Vælg nu, for de givne primtal, $h := np_1 \cdots p_k$. Tallet $\Phi_n(h)$ er større end 1, så der findes et primtal p , med $p \mid \Phi_n(h)$. Da $\Phi_n(h)$ er divisor i $h^n - 1$, er p divisor i $h^n - 1$. Specielt kan p ikke være divisor i h . Altså er p forskellig fra de givne primtal, og p er ikke divisor i n . Modulo p er restklassen $[h] \in \mathbb{F}_p$ rod i Φ_n . Følgelig har $[h]$ orden n i gruppen $\mathbb{F}_p^*$. Altså er n divisor i $p - 1$, dvs $p \equiv 1 \pmod{n}$, som ønsket.

Det er en sætning af Dirichlet, at der i enhver primisk restklasse findes uendelig mange primtal, altså at der for hvert a primisk med n findes uendelig mange primtal p med $p \equiv a \pmod{n}$. Ovenstående viser resultatet for $a = 1$.

(3.16) Bemærkning. Lad os som yderligere anvendelse vise, at ethvert endeligt skævlegeme Λ er kommutativt [Wedderburn's Sætning, 1905].

Hertil betragtes centret L i Λ , bestående af de elementer $\alpha \in \Lambda$, som kommuterer med alle $\lambda \in \Lambda$. Øjensynlig er L et kommutativt dellegeme af Λ . Specielt er elementantallet i L en primtalspotens q . Som i (3.9) kan vi opfatte Λ som vektorrum over L . Specielt følger det, at elementantallet i Λ er en potens q^r af q . Det skal vises, at $r = 1$.

Den multiplikative gruppe Λ^* har orden $q^r - 1$. Det er klart, at L^* er centret i gruppen Λ^* . Klasseformlen har altså formen,

$$q^r - 1 = q - 1 + \sum' |\Lambda^* : C^*(\alpha_j)|, \quad (3.16.1)$$

hvor $C^*(\alpha)$ er centralisatoren i Λ^* af α , og summen er over repræsentanter for konjugeret-klasser uden for centret. Specielt er hvert led i summen strengt større end 1. Centralisatoren $C^*(\alpha)$ består af de elementer $\lambda \in \Lambda^*$, for hvilke $\lambda\alpha = \alpha\lambda$. Føjes hertil nul-elementet, fremkommer øjensynlig et delskævlegeme $C(\alpha)$ af Λ . Da $L \subseteq C(\alpha)$, følger det at $|C(\alpha)|$ er en potens q^d . Altså er $|C^*(\alpha)| = q^d - 1$.

Klasseformlen giver altså en ligning af formen,

$$q^r - 1 = q - 1 + \sum \frac{q^r - 1}{q^{d_j} - 1}.$$

Hvert led i summen er et helt tal, så $q^{d_j} - 1 \mid q^r - 1$. Heraf følger let, at $d_j \mid r$. Endvidere er d_j en ægte divisor i r , da leddene i summen var større end 1. Det følger nu af (3.3.1), at tallet $\Phi_r(q)$ er divisor i hvert led i summen. Videre er $\Phi_r(q)$ divisor i $q^r - 1$. Af ligningen følger derfor, at $\Phi_r(q)$ er divisor i $q - 1$. Vurderingen (3.15.1) giver nu en modstrid, med mindre $r = 1$.

(3.17) Opgaver.

- H2 1. Vis, at konstantleddet i Φ_n , for $n > 1$, er lig med 1. Vis, at koefficienterne i Φ_n ikke altid er ± 1 eller 0. [Vink: bestem nogle koefficienter i Φ_{105} .]
- U4 2. Vis for $\zeta \in \mathbb{C}$ og et ulige tal u , at ζ har orden $2u$, hvis og kun hvis $-\zeta$ har orden u . Slut heraf, at $\Phi_{2u}(X) = \Phi_u(-X)$.
- U4 3. For et polynomium f af grad k defineres $c(f) := -f_{k-1}$, hvor f_{k-1} er koefficienten til leddet af næsthøjeste grad. Vis, for normerede polynomier f, g , at $c(fg) = c(f) + c(g)$. Vis, at næsthøjestegrads-koefficienten i Φ_n er lig med $-\mu(n)$, hvor $\mu(n)$ er Möbius-funktionen. [Vink: Brug Opgave Kap1: 1.]
- U4 4. Vis formen $\Phi_n = \prod_{d \mid n} (X^{n/d} - 1)^{\mu(d)}$, hvor μ er Möbius-funktionen.
- U4 5. Det fremgår af Eksempel (3.12), at i $\mathbb{F}_7[X]$ er $f := X^2 + X - 4$ divisor i Φ_{48} . Bestem kvotienten Φ_{48}/f .
6. Angiv, i $\mathbb{F}_7[X]$, primopløsningen af Φ_{48} (eller i hvert fald nogle af primfaktorerne).
- U5 7. Diskuter for hvilke n og primtal $p \nmid n$ polynomiet Φ_n er irreducibelt i $\mathbb{F}_p[X]$. (Fx: Findes der for et givet n altid sådanne primtal p ? Eventuelt uendelig mange?)
8. Bestem Φ_{28} .
- U4 9. Vis, når p er et primtal og $p \nmid n$, at $\Phi_{np}(X) = \Phi_n(X^p)/\Phi_n(X)$.
- U4 10. Vis, når p er et primtal og $p \nmid n$, at i $\mathbb{F}_p[X]$ er $\Phi_{np} = \Phi_n^{p-1}$.
- U5 11. Vis, at der for $\mathbb{F}_p[X]$ gælder, at brøkdelen af irreducible polynomier blandt alle polynomier af grad n asymptotisk er lig med $1/n$.
- U9 12. *Vis „primtalssætningen“ for $\mathbb{F}_p[X]$: Nummerér polynomierne i $\mathbb{F}_p[X]$, således at først kommer konstanterne, dernæst polynomierne af grad 1, dernæst polynomierne af grad 2, osv; polynomierne af samme grad nummereres tilfældigt. Lad $\pi_p(n)$ være antallet af irreducible blandt de første n polynomier. Da gælder asymptotisk: $\pi_p(n) \sim Cn/\log n$, med konstanten $C = \log p$.
- U4 13. Vis, at hvis $q^d - 1$ er divisor i $q^s - 1$, så er $d \mid s$. [Vink: skriv $s = hd + r$, med $r < d$, og regn modulo $q^d - 1$.]
- U4 14. Vis, for enhedsrødderne $\zeta_5 := e^{2\pi i/5}$ og $\zeta_{10} := e^{2\pi i/10}$, at

$$\zeta_5 = \frac{\sqrt{5}-1}{4} + i \frac{\sqrt{10+2\sqrt{5}}}{4}, \quad \zeta_{10} = \frac{\sqrt{5}+1}{4} + i \frac{\sqrt{10-2\sqrt{5}}}{4}.$$

[Vink: $\zeta := \zeta_5$ er rod i Φ_5 , så $\zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0$. Efter division med ζ^2 fås $0 = (\zeta + \zeta^{-1})^2 + (\zeta + \zeta^{-1}) - 1$, hvoraf $\zeta + \zeta^{-1} = \frac{-1 \pm \sqrt{5}}{2}$. Tilsvarende er ζ_{10} rod i $\Phi_{10} = X^4 - X^3 + X^2 - X + 1$.]

- U6 15. Der er velkendte „pæne“ udtryk for de primitive n 'te enhedsrødder ζ_n for $n = 3, 4$ og 5 . Ud fra et udtryk $\zeta_n = a + ib$ ($b > 0$) får man et udtryk for ζ_{2n} ved at løse andengradsligningen $z^2 = a + ib$; det giver

$$\zeta_{2n} = \sqrt{\frac{\sqrt{a^2 + b^2} + a}{2}} + i\sqrt{\frac{\sqrt{a^2 + b^2} - a}{2}} = \sqrt{\frac{1+a}{2}} + i\sqrt{\frac{1-a}{2}}.$$

Bestem herved pæne udtryk for $\zeta_6, \zeta_8, \zeta_{10}, \zeta_{12}, \zeta_{16}, \zeta_{20}, \zeta_{24}$. Hvorfor kan man ikke tilsvarende få et udtryk for ζ_9 , og mere generelt for ζ_{3n} , ved at bruge, at $z = \zeta_{3n}$ opfylder $z^3 = a + ib$? – det er jo en simpel trediegradsligning, og Cardano's formel fortæller, hvordan sådan en skal løses.

- U6 16. Vis, når p er et primtal og $p \mid m$, at $\Phi_{p^v m}(X) = \Phi_m(X^{p^v})$. Vis, når $p \nmid n$ og $v > 0$, at $\Phi_{p^v n}(X) = \Phi_n(X^{p^v}) / \Phi_n(X^{p^{v-1}})$.

- U6 17. Principielt kan n 'te enhedsrødder defineres i en vilkårlig (kommutativ) gruppe G : Det er de elementer $g \in G$, som opfylder, at $g^n = 1$. Lad $\alpha_G(n)$ betegne antallet af n 'te enhedsrødder. Hvordan bestemmer man antallet af elementer af orden n ud fra funktionen α_G ?

Hvordan bestemmer man $\alpha_G(n)$, når G er cyklisk? Hvordan bestemmes antallet $\alpha_{G \times H}(n)$ for en produktgruppe ud fra α_G og α_H ?

- U8 18. Lad K være et endeligt legeme af karakteristisk p . Vis, at elementantallet q i K er en potens $q = p^r$ af p . Vis, at $\alpha^q = \alpha$ for alle $\alpha \in K$.

19. Lad L være et legeme af positiv karakteristisk p . Afbildningen $\sigma(\xi) := \xi^p$ er så en ringhomomorfi $\sigma: L \rightarrow L$, og den inducerer en ringhomomorfi $L[X] \rightarrow L[X]$, hvor billedet ${}^\sigma f$ af et polynomium $f \in L[X]$ fås ved at anvende σ på koefficienterne i f .

Lad f være et normeret polynomium med koefficienter i $\mathbb{F}_p$. Vis, at hvis f i L har en rod ξ , så er også ξ^p rod i f .

Antag, at $f \in \mathbb{F}_p[X]$ er irreducibelt, med roden ξ i L , og at $f \neq X$ (altså at $\xi \neq 0$). Lad r være graden af f og lad n være ordenen af ξ . Da gælder som bekendt, at r er ordenen af restklassen af p modulo n . Vis, at rødderne i f er potenserne ξ^{p^i} for $i = 0, \dots, r-1$.

- U6 20. Antag, at $p \equiv 3 \pmod{4}$ er et primtal. Vis, at legemet $\mathbb{F}_{p^2}$, med p^2 elementer, så kan defineres som kvotienten $\mathbb{F}_p[X]/(X^2 + 1)$. Idet i betegner restklassen af X , har elementerne α i $\mathbb{F}_{p^2}$ altså fremstillinger $\alpha = a + ib$ med entydigt bestemte koefficienter $a, b \in \mathbb{F}_p$. Regning i $\mathbb{F}_{p^2}$ er bestemt ved $i^2 = -1$.

Vis, at $\alpha = a + ib$ er rod i polynomiet $(X - a)^2 + b^2 \in \mathbb{F}_p[X]$. Sæt $\bar{\alpha} := a - ib$. Vis, at $\alpha \mapsto \bar{\alpha}$ er en ringhomomorfi $\mathbb{F}_{p^2} \rightarrow \mathbb{F}_{p^2}$. Vis, at $\bar{\alpha} = \alpha^p$ for alle $\alpha \in \mathbb{F}_{p^2}$.

- U6 21. Legemet $\mathbb{F}_{49}$ er beskrevet i (3.12): Elementerne har formen $a + ib$, hvor $a, b \in \mathbb{F}_7$ og $i^2 = -1$. For elementet $\xi = 5 + 3i$ er $\xi^2 = 2 + 2i$, og $\xi^4 = i$. Specielt er $\xi^8 = -1$ og ξ har orden 16. Elementet $\zeta = 2\xi = 3 - i$ har så orden 48.

Bestem de 8 potenser ζ^a for $a = 1, 5, 11, 13, 17, 19, 25, 41$, og de 8 normerede andengradspolynomier i $\mathbb{F}_7[X]$, hvori potenserne er rødder. Hvad kan du sige om disse polynomier i relation til cirkeldelingspolynomiet Φ_{48} .

30. september 2009

22. *Lad p være et ulige primtal. Vis, at der findes en ring med præcis p enheder, hvis og kun hvis p er et Mersenne-primtal.
23. Vis, at Sætning (3.8) gælder, når $\mathbb{F}_p$ erstattes med et vilkårligt endeligt legeme L med q elementer: Antag $(n, q) = 1$. Betragt i $L[X]$ en irreducibel divisor f i Φ_n . Så er f 's grad lig med ordenen af $[q]_n$ i $(\mathbb{Z}/n)^*$.
24. Vis, at Φ_{17} er irreducibel i $\mathbb{F}_3[X]$.