Eötvös Loránd Tudományegyetem
Természettudományi Kar

Egy általánosabb reciprocitási tétel

Seress Dániel

BSc Szakdolgozat

Témavezető:
Zábrádi Gergely, adjunktus

Algebra és Számelmélet Tanszék

Budapest, 2019

Tartalomjegyzék

Köszönetnyilvánítás **4**

Bevezetés **5**

1. Előismeretek **7**
1.1. Néhány számelméleti függvény 7
1.2. $\mathbb{Z}$ maradékosztálygyűrűi 7
1.3. Végtelen sok prímszám bizonyos halmazokban 9
1.4. Többváltozós polinomok 10
1.5. Polinomok diszkriminánsa 11
1.6. Algebrai testbővítések 11
1.7. Normális bővítések 12
1.8. Szeparábilis bővítések 13
1.9. Galois-csoport 14
1.10. Véges testek 16

2. Egységgyökök és körosztási polinomok **18**
2.1. Egységgyökök és körosztási testek 18
2.2. Körosztási polinomok 20
2.3. Végtelen sok prím bizonyos halmazokban 23

3. Másodfokú polinomok és a kvadratikus reciprocitás tétele **25**

4. Egy általánosabb reciprocitási tétel **26**
4.1. Bevezetés 26
4.1.1. A polinom megadása a gyökei által 26
4.1.2. Kitüntetett esetek 27
4.1.3. A polinom egész együtthatós és irreducibilis az egészek fölött 27
4.1.4. A polinom igazzá teszi a reciprocitási tételt 28
4.2. A polinom (együtthatóinak) kiszámítása 29
4.3. A kvadratikus reciprocitás tételének a bizonyítása 32
4.4. A kivételes prímek vizsgálata 33

Köszönetnyilvánítás

Köszönöm a témavezetőmnek, Zábrádi Gergelynek, hogy az Algebra szemináriumon elmondott állításomat érdemesnek találta egy szakdolgozat keretében való megírásra, és később is hasznos információkkal, szempontokkal segített.

Köszönöm az Algebra szeminárium oktatóinak, hogy a szemináriumon ösztönözték a hallgatók saját állításait és kérdéseit.

Köszönöm Pálfy Péter Pálnak, hogy Gauss feljegyzését idézve megerősítette az állításom egy konkrét esetének számadatára vonatkozó sejtésemet.

Köszönöm Sárközy Andrásnak, hogy a Számelmélet 1 előadáson elmondta néhány egyszerűbb halmazról, hogy végtelen sok prím van bennük. Ettől érdekelni kezdett az általánosítás lehetősége.

Köszönöm Kós Gézának a 2018-as Schweitzer-verseny 6. feladatának kitűzését, amely az állításom nehéz irányának bizonyítása volt egy konkrét esetben. Ezzel ösztönözve voltam a gondolataim rendezett leírására.

Köszönöm a szüleimnek, hogy az egyetemi éveim alatt támogattak, segítettek, biztos hátteret jelentettek számomra.

Bevezetés

Mely p prímekre oldható meg egy egész együtthatós, $\mathbb{Q}$ fölött irreducibilis polinom modulo p? Mely p prímekre bomlik gyöktényezőkre modulo p? (Mikor ekvivalens ez a két feltétel?)

Van olyan irreducibilis polinom, amely esetén valamilyen n-re ezen prímek modulo n maradékosztályai csoportot alkotnak. Ilyen például minden elsőfokú polinom triviálisan, minden másodfokú polinom a megoldóképlet és a kvadratikus reciprocitás tétele miatt, ill. a körosztási polinomok.

A szakdolgozatban belátom, hogy adott n-re bármely $H \leq \mathbb{Z}_n^*$ részcsoport "majdnem" megkapható a fenti módon, vagyis van olyan $f_{n,H}$ irreducibilis polinom, amely véges sok kivétellel pontosan akkor oldható meg, ill. bomlik gyöktényezőkre modulo p, ha $p \in H$ modulo n. (Ha a polinomnak van gyöke modulo p, akkor véges sok kivétellel gyöktényezőkre is bomlik modulo p.)

Az $f_{n,H}$ polinomot a gyökei által adom meg, a gyököket pedig a primitív n-edik egységgyökök olyan összegeiként, hogy H hatása a primitív n-edik egységgyökökön $f_{n,H}$ minden gyökét fixálja. A definíciót felhasználva $\mathbb{Z}_n^*/H$ egy természetes reprezentációja $f_{n,H}$ Galois-csoportjának.

A polinom foka a fenti példákhoz hasonlóan általában is egyenlő a részcsoport indexével. Kezdetlegesen jellemzem a kivételes prímeket. Belátom, hogy bizonyos maradékosztályok uniójában végtelen sok prím van (ez a Dirichlet-tétel bizonyos speciális eseteit, ill. gyengítéseit jelenti).

Az 1. fejezet a téma kifejtéséhez szükséges számelméleti és testelméleti előismeretek összefoglalása.

A 2. fejezet a test fölötti egységgyökök és a körosztási polinomok általános, tisztán algebrai konstrukciója. Ez azért érdekelt, mert a komplex test valós fölötti 2 dimenziós reprezentációjában az egységgyökök mint a teljesszög racionális többszöröseivel való forgatások eleve adottak. Így a racionális test egységgyökökkel való bővíthetősége (legalábbis szemléletesen, még ha formálisan nem is) a valós számok létezésén és a teljesszög tetszőleges részekre oszthatóságán múlik (akkor is, ha a keletkező forgásszögek algebrai számokat reprezentálnak).

A körosztási polinomok az általánosan tárgyalt polinom egyik legfontosabb speciális esete.

A 3. fejezet a másodfokú polinomok és a kvadratikus reciprocitás tétele mint speciális eset leírása.

A 4. fejezet a polinom általános tárgyalása, majd a 3. fejezetben kimondott kvadratikus reciprocitási tétel bizonyítása az általános tétel felhaszná-

lásával.

Bizonyos fogalmakat (körosztási test, körosztási polinom, Legendre-szimbólum) a szokásostól eltérő módon definiálok, úgy, hogy a definíció az általam elsősorban használt, lényegesnek tartott tulajdonságot mutassa meg.

A szakdolgozat témája elsősorban a testelmélet (azon belül a Galois-elmélet) területéhez tartozik. A felhasznált állítások tárgyalásának részletessége ennek megfelelő:

A testelméleti állításokat külön kimondom és többnyire bizonyítom (ahol a bizonyítás nem túl hosszú vagy túl technikai). A számelméleti és gyűrűelméleti állításokat külön kimondom, de nem bizonyítom. A csoportelméleti állításokat nem mondom ki külön, csak hivatkozom rájuk bizonyítás közben.

Jelölések és megállapodások a dolgozat teljes szövegében:

n, m pozitív egész számok

p, q pozitív prímszámok

modulo p = $\mathbb{F}_p$-ben

K, L testek, $L|K$ testbővítés

Ha egy újonnan bevezetett számról feltesszük, hogy egész (pl. prímszám, osztója egy számnak, osztható egy számmal, stb.) és nem mondunk róla mást, akkor mindig pozitív egészre gondolunk.

1. Előismeretek

1.1. Néhány számelméleti függvény

1.1.1. Definíció (Relatív prímek száma). Az n-nél nem nagyobb, n-hez relatív prím pozitív egészek számát $\varphi(n)$-nel jelöljük. Ez a függvény az Euler-féle φ-függvény.

1.1.2. Definíció (Különböző prímosztók száma). Az n szám különböző (pozitív) prímosztóinak számát $\omega(n)$-nel jelöljük.

1.1.3. Definíció (Különböző prímosztók szorzata). Az n szám különböző (pozitív) prímosztóinak szorzatát az n radikáljának mevezzük, és $rad(n)$-nel jelöljük.

1.1.4. Definíció (Möbius-függvény). A Möbius-függvény a következő, pozitív egész számokon értelmezett függvény:
$\mu(n) = (-1)^{\omega(n)}$, ha n négyzetmentes, és $\mu(n) = 0$, ha n nem négyzetmentes.

1.1.5. Tétel. Legyen $n > 1$. Ekkor $\sum_{m|n} \mu(m) = 0$.

Bizonyítás. $n > 1$-re $\omega(n) > 0$. n-nek minden $l = 0, 1, ..., \omega(n)$-re $\binom{\omega(n)}{l}$ db olyan m négyzetmentes osztója van, amelyre $\omega(m) = l$. Ezért az összeg:

$$\sum_{m|n} \mu(m) = \sum_{m|rad(n)} \mu(m) = \sum_{l=0}^{\omega(n)} (-1)^l \cdot \binom{\omega(n)}{l} = (1-1)^{\omega(n)} = 0^{\omega(n)} = 0$$

□

1.1.6. Definíció (Kronecker-delta függvény). $\delta_{i,j} = 1$, ha $i = j$, és $\delta_{i,j} = 0$, ha $i \neq j$

1.2. $\mathbb{Z}$ maradékosztálygyűrűi

1.2.1. Definíció. A $\mathbb{Z}/n\mathbb{Z}$ faktorgyűrűt $\mathbb{Z}_n$-nel jelöljük. A $\mathbb{Z}_n$ gyűrű összeadását, ill. szorzását az egész számok modulo n összeadásának, ill. szorzásának is nevezzük.

1.2.2. Tétel. 1.1.5 $|\mathbb{Z}_n^*| = \varphi(n)$.

1.2.3. Tétel. $\mathbb{Z}_n$ pontosan akkor nullosztómentes, ha n prím, és ekkor test is.

Bizonyítás. Ha $n = ab$, ahol $1 < a, b < n$, akkor $a \cdot b = n \equiv 0$ modulo n, tehát $a, b \in \mathbb{Z}_n$ nullosztók.

Ha $n = p$ és $0 < a < p$, akkor a $0, a, ..., (p-1)a$ egész számok páronként inkongruensek modulo p, mert bármely $k, l \in \{0, ..., p-1\}, k \neq l$-re $ka - la = (k-l)a$, ahol $1 \leq |k-l| \leq p-1$, vagyis $p \nmid (k-l)a$. Ezért valamilyen $k \in \{1, ..., p-1\}$-re $ka \equiv 1$ modulo p. Vagyis minden $0 \neq a \in \mathbb{Z}_n$-nek van inverze, tehát $\mathbb{Z}_n$ test. □

1.2.4. Tétel. Ha $\gcd(m, n) = 1$, akkor $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$ és $\mathbb{Z}_{mn}^* \simeq \mathbb{Z}_m^* \times \mathbb{Z}_n^*$.

1.2.5. Tétel. Ha $p > 2$ prím és $l > 0$ egész, akkor $\mathbb{Z}_{p^l}^* \simeq Z_{p^{l-1}(p-1)}$.

Bizonyítás. l szerinti indukcióval belátjuk, hogy ha $l \geq 2$, akkor

$$(p+1)^{p^{l-2}} \equiv p^{l-1} + 1 \mod p^l$$

$l = 2$-re triviális:

$$p + 1 \equiv p + 1 \mod p^2$$

Tegyük fel, hogy $l \geq 3$, és $l-1$-re már tudjuk, vagyis

$$(p+1)^{p^{l-3}} \equiv p^{l-2} + 1 \mod p^{l-1}$$

Ekkor

$$(p+1)^{p^{l-2}} = ((p+1)^{p^{l-3}})^p \equiv (p^{l-2} + 1)^p \mod p^{l-1}$$

és

$$(p^{l-2} + 1)^p \equiv \binom{p}{2} \cdot p^{2l-4} + p \cdot p^{l-2} + 1 \mod p^l$$

$$\binom{p}{2} \cdot p^{2l-4} = \frac{p(p-1)}{2} \cdot p^{2l-4} = \frac{p-1}{2} \cdot p^{2l-3}$$

és ez $2l - 3 \geq l$ miatt osztható p^l-lel. Tehát

$$(p^{l-2} + 1)^p \equiv p \cdot p^{l-2} + 1 = p^{l-1} + 1 \mod p^l$$

és

$$(p+1)^{p^{l-1}} = ((p+1)^{p^{l-2}})^p \equiv (p^{l-1} + 1)^p \equiv p \cdot p^{l-1} + 1 = p^l + 1 \equiv 1 \mod p^l$$

Ezért $o_{p^l}(p+1) = p^{l-1}$.

$l = 1$-re triviális. Tegyük fel, hogy $l \geq 2$, és tudjuk, hogy $o_{p^{l-1}}(p+1) = p^{l-2}$. Ekkor

$(p+1)^{p^{l-1}} \equiv 1 \mod p^l$.

$$(p+1)^{p^{l-1}} = ((p+1)^{p^{l-2}})^p \equiv ((p+1)^{p^{l-2}})^p \equiv 1 \mod p^l$$

$$p+1 \equiv p+1 \mod p^2$$
$$(p+1)^p \equiv p^2+1 \mod p^3$$
$$(p^2+1)^p \equiv p^3+1 \mod p^4$$
$$(p+1)^{p^2} \equiv p^3+1 \mod p^4$$
$$(p^{l-1}+1)^p \equiv p \cdot p^{l-1} + 1 = p^l + 1 \equiv 1 \mod p^l$$

$$(p+1)^p \equiv \binom{p}{2} \cdot p^2 + p \cdot p + 1 \equiv p^2 + 1 \mod p^3$$
$$(p^2+1)^p \equiv \binom{p}{2} \cdot p^4 + p \cdot p^2 + 1 \equiv p^3 + 1 \mod p^4$$
$$(p^{l-2}+1)^p \equiv \binom{p}{2} \cdot p^{2(l-2)} + p \cdot p^{l-2} + 1 \equiv p^{l-1} + 1 \mod p^l$$

□

1.2.6. Tétel. Ha $l > 1$ egész, akkor $\mathbb{Z}_{2^l}^* \simeq Z_2 \times Z_{2^{l-2}}$.

1.3. Végtelen sok prímszám bizonyos halmazokban

Prímek bizonyos halmazainak végtelenségét bizonyítjuk. Legyen $A \subseteq \mathbb{Z}_+$. A bizonyításokhoz a következő egyszerű tételt használjuk:

1.3.1. Tétel. Ha minden N egészhez van olyan A-beli prím, amely nem osztója N-nek, akkor A-ban végtelen sok prím van.

Bizonyítás. Ha A-ban véges sok prím van, akkor a szorzatuk mindegyikkel osztható. □

Ezért a következő tételek bizonyítása során azt látjuk be, hogy bizonyos A halmazok esetén minden N egészhez van olyan A-beli prím, amely nem osztója N-nek. Ezt általában a következőképpen csináljuk:

N-hez választunk egy olyan $k > 1$ számot, amelyre $\gcd(N, k) = 1$, és teljesül rá egy bizonyos, A-tól függő feltétel. k-nak van prímosztója. k semmilyen prímosztója nem osztja N-et, és van köztük A-beli (ehhez kell az A-tól függő feltétel).

1.3.2. Tétel ($A = \mathbb{Z}_+$)**.** Végtelen sok prímszám van.

Bizonyítás. Legyen N egész szám. $N + 1 > 1$ miatt $N + 1$-nek van prímosztója, és $N + 1$ semmilyen prímosztója nem osztja N-et. Ebből következik, hogy végtelen sok prím van. □

1.3.3. Tétel (A végtelen és $\mathbb{Z}_+ \setminus A$ zárt a szorzásra)**.** Legyen $n \in \mathbb{Z}_+$, $K \lneq \mathbb{Z}_n^*$. (Ebből következik $n \geq 3$.) Ekkor végtelen sok olyan prím van, amely $\mathbb{Z}_n^* \setminus K$-beli modulo n.

Bizonyítás. Legyen N egész szám. Ekkor a kínai maradéktétel miatt van olyan $k > 1$ egész szám, amelyre $\gcd(N, k) = 1$ és $k \in \mathbb{Z}_n^* \setminus K$ modulo n. Ekkor k semmilyen prímosztója nem osztja N-et és n-et, és van köztük $\mathbb{Z}_n^* \setminus K$-beli modulo n. Ebből következik, hogy végtelen sok olyan prím van, amely $\mathbb{Z}_n^* \setminus K$-beli modulo n. □

1.4. Többváltozós polinomok

1.4.1. Definíció (Lexikografikus sorrend)**.** Két n-változós monom közül az a lexikografikusan nagyobb, amelyikben az első, a két tagban különböző kitevőn szereplő változó kitevője nagyobb (az együtthatókat nem vesszük figyelembe).

$$x_1^{a_1}...x_n^{a_n} \prec x_1^{b_1}...x_n^{b_n} \Leftrightarrow \exists k \in \{1, ..., n\} : a_1 = b_1, ..., a_{k-1} = b_{k-1}, a_k < b_k$$

A $\prec$ reláció irreflexív, antiszimmetrikus és tranzitív. Bármely két monom közül az egyik lexikografikusan kisebb. Tehát $\prec$ rendezés a monomok halmazán.

Egy többváltozós polinom lexikografikusan legnagyobb tagját a polinom vezető tagjának nevezzük. Két polinom közül az a lexikografikusan nagyobb, amelynek a vezető tagja nagyobb. így részbenrendezést kapunk $R[x_1, ..., x_n]$ fölött. Ezt lexikografikus rendezésnek nevezzük.

1.4.2. Definíció (Szimmetrikus polinomok). Az $x_1, ..., x_n$ változók $f(x_1, ..., x_n) \in R[x_1, ..., x_n]$ polinomja szimmetrikus, ha minden $\pi \in S_n$ permutációra $f(x_{1\pi}, ..., x_{n\pi}) = f(x_1, ..., x_n)$. Az $x_1, ..., x_n$ változók szimmetrikus polinomjai részgyűrűt alkotnak $R[x_1, ..., x_n]$-ben.

1.4.3. Definíció (Elemi szimmetrikus polinomok). Ha $k = 1, ..., n$, akkor az $x_1, ..., x_n$ változók k-adik elemi szimmetrikus polinomja:

$$\sigma_k(x_1, ..., x_n) = \sum \prod x$$

1.4.4. Tétel (Szimmetrikus polinomok alaptétele). Minden szimmetrikus polinom egyértelműen előáll az elemi szimmetrikus polinomok polinomjaként.

Bizonyítás. □

1.5. Polinomok diszkriminánsa

1.5.1. Definíció (Diszkrimináns). Legyen $f(x) = \sum_{k=0}^{n} a_k x^k \in K[x]$ n-edfokú, a_n főegyüttható polinom, és legyen egy alkalmas bővebb testben $f(x) = a_n \prod_{j=1}^{n}(x - \alpha_j)$. Ekkor az $a_n^{2n-2} \prod_{1 \le i < j \le n}(\alpha_i - \alpha_j)^2$ számot f diszkriminánsának nevezzük és $D(f)$-fel jelöljük. Nyilván $D(f)$ pontosan akkor 0, ha f-nek van többszörös gyöke.

1.5.2. Tétel. Ha $f \in K[x]$, akkor $D(f) \in K$.

Bizonyítás. $D(f)$ az f gyökeinek homogén szimmetrikus polinomja. Tehát a szimmetrikus polinomok alaptétele szerint előáll az f gyökei elemi szimmetrikus polinomjainak polinomjaként.

Viszont az f gyökeinek a k-adik elemi szimmetrikus polinomja a megfelelő Viète-formula szerint éppen $(-1)^k a_{n-k}$. Vagyis $D(f)$ előáll az f együtthatóinak polinomjaként, vagyis K-beli. □

1.6. Algebrai testbővítések

Legyen $L|K$ testbővítés.

1.6.1. Definíció (Algebrai elem). $\alpha \in L$ algebrai K fölött, ha van olyan K fölötti polinom, amelynek α gyöke.

1.6.2. Definíció (Algebrai bővítés). $L|K$ algebrai, ha L minden eleme algebrai K fölött.

1.6.3. Definíció (Egyszerű bővítés). Az $L|K$ bővítés egyszerű, ha van olyan $\alpha \in L$, amelyre $L = K(\alpha)$.

Legyen $f \in K[x]$ polinom.

1.6.4. Definíció (Felbontási test). $L|K$ felbontási teste f-nek, ha f gyöktényezőkre bomlik L-ben, vagyis $f(x) = a \cdot \prod_{j=1}^{n}(x-\alpha_j)$, és $L = K(\alpha_1, ..., \alpha_n)$.

1.6.5. Tétel (Felbontási test létezése). f-nek létezik felbontási teste K fölött.

Bizonyítás. Legyen $\deg f = n$ és legyen f-nek k gyöke K-ban.

Bontsuk f-et irreducibilis tényezőkre K fölött, és legyen az egyik tényező g_1. Adjungáljuk K-hoz g_1 egy gyökét, így kapjuk L_1-et. Itt f-nek már legalább $k+1$ gyöke van.

Folytassuk ezt addig, amíg a kapott L_m testben f-nek már n gyöke van. Itt f már gyöktényezőkre bomlik: $f(x) = a \cdot \prod_{j=1}^{n}(x - \alpha_j)$.

Vegyük $L_m|K$-ban a $K(\alpha_1, ..., \alpha_n)$ résztestet. Ez minimális arra, hogy fölötte f gyöktényezőkre bomlik. Véges sok véges bővítés egymásutánja, ezért véges. □

1.7. Normális bővítések

1.7.1. Definíció (Normális bővítés). Az $L|K$ algebrai bővítés normális, ha minden K fölötti polinom, amelynek van gyöke L-ben, $L[x]$-ben gyöktényezőkre bomlik.

1.7.2. Tétel. Az $L|K$ véges bővítés pontosan akkor normális, ha izomorf egy $f \in K[x]$ felbontási testével.

Bizonyítás. Legyen L a normált $f \in K[x]$ polinom felbontási teste, azaz $L = K(\alpha_1, ..., \alpha_n)$, ahol $f(x) = a \cdot \prod_{j=1}^{n}(x - \alpha_j)$. Legyen g olyan K fölötti irreducibilis polinom, amelynek gyöke $\beta \in L$. Belátjuk, hogy g gyöktényezőkre bomlik L fölött. $\beta = g(\alpha_1, ..., \alpha_n)$, ahol $g \in K[_1, ..._n]$. Tekintsük az alábbi polinomot:

$$h(x) = \prod_{\sigma \in S_n} (x - g(\alpha_{1\sigma}, ..., \alpha_{n\sigma}))$$

Ennek együtthatói az $\alpha_1, ..., \alpha_n \in L$ szimmetrikus polinomjai K-beli együtthatókkal, mert a definíció szimmetrikus és $g \in K[_1, ...,_n]$. A szimmetrikus polinomok alaptétele szerint $h(x)$ előáll $\alpha_1, ..., \alpha_n$ elemi szimmetrikus polinomjainak, azaz g együtthatóinak K fölötti polinomjaként. Tehát $h(x) \in K[x]$. $h(\beta) = 0$, mert $h(x)$ definíciójában σ-t az identikus permutációnak választva a megfelelő tényező $x - \beta$. β kanonikus polinomja g, ezért $g \mid h$ $K[x]$-ben. Ekkor $L[x]$-ben is, tehát g $L[x]$-beli irreducibilis tényezői h irreducibilis tényezői közül valók, vagyis gyöktényezők.

L véges bővítés, ezért előáll $K(\alpha_1, ..., \alpha_n)$ alakban. Legyen α_j kanonikus polinomja g_j. Mindegyik g_j polinom irreducibilis $K[x]$-ben és van gyöke L-ben. Ha $L|K$ normális, akkor mindegyik gyöktényezőkre bomlik, így a szorzatuk, $h(x) = \prod_{j=1}^{n} g_j(x)$ is. állítsuk elő h felbontási testét úgy, hogy K-hoz először $\alpha_1, ..., \alpha_n$-et adjungáljuk, majd a többi gyökét. így h felbontási testét kapjuk K fölött, ami L, mert h minden gyöke L-beli. □

1.8. Szeparábilis bővítések

1.8.1. Definíció. Az $f \in K[x]$ irreducibilis polinom szeparábilis, ha felbontási testében minden gyöke egyszeres. Inszeparábilis, ha van többszörös gyöke.

1.8.2. Tétel. Az $f \in K[x]$ irreducibilis polinom pontosan akkor inszeparábilis, ha $char(K) = p$ prím, és $f(x) = \sum_{k=0}^{m} a_{kp} x^{kp}$.

Bizonyítás. Legyen $f(x) = \sum_{k=0}^{n} a_k x^k$ irreducibilis és inszeparábilis. Ekkor van többszörös gyöke, vagyis van közös gyöke a deriváltjával. Ekkor $\gcd(f, f')$ nem konstans polinom. f irreducibilitása miatt $\gcd(f, f') = f$, vagyis $f \mid f'$, így $\deg f' < \deg f$ miatt $f' \equiv 0$. $0 \equiv f' = \sum_{k=1}^{n} k \cdot a_k x^{k-1}$ miatt $k \cdot a_k = 0$ minden $k = 1, ..., n$-re. Ha $char(K) = 0$, akkor $n \cdot a_n \neq 0$. Tehát $char(K) = p$ prím, és f-nek csak a p-hatvány fokú együtthatói nem 0-k.

A fenti implikációk mind megfordíthatóak, ezért ha $char(K) = p$ prím, akkor minden $f(x) = \sum_{k=0}^{m} a_{kp} x^{kp}$ alakú irreducibilis polinom inszeparábilis. □

1.8.3. Definíció. Legyen α algebrai K fölött. α szeparábilis, ha a kanonikus polinomja szeparábilis.

1.8.4. Definíció. Az $L|K$ algebrai bővítés szeparábilis, ha minden eleme szeparábilis.

1.8.5. Definíció. Az $f \in K[x]$ polinom szeparábilis, ha minden irreducibilis tényezője szeparábilis.

1.8.6. Definíció. A K test perfekt, ha minden irreducibilis polinomja szeparábilis. Ekvivalensen:
minden polinomja szeparábilis;
minden véges bővítése szeparábilis;
minden algebrai bővítése szeparábilis;
minden fölötte algebrai elem szeparábilis.

1.8.7. Tétel. Minden 0 karakterisztikájú test perfekt.

Legyen $char(K) = p$ prím. Ekkor K pontosan akkor perfekt, ha K minden elemének van p-edik gyöke K-ban.

Bizonyítás. Az előző tétel szerint 0 karakterisztikájú test fölött nincs inszeparábilis irreducibilis polinom.

Tegyük fel, hogy $char(K) = p$ prím, és K minden elemének van p-edik gyöke K-ban. Ha f inszeparábilis, akkor $f(x) = \sum_{k=0}^{m} a_{kp}x^{kp}$. Legyen minden $k = 0, ..., m$-re $c_k^p = a_{kp}$. Ekkor

$$f(x) = \sum_{k=0}^{m} a_{kp}x^{kp} = \sum_{k=0}^{m} c_k^p x^{kp} = (\sum_{k=0}^{m} c_k x^k)^p$$

Vagyis f nem irreducibilis, ezért nem inszeparábilis. Tegyük fel, hogy $a \in K$-nak nincs p-edik gyöke K-ban. Legyen $f(x) = x^p - a$, f felbontási teste L, $\alpha \in L$ gyöke f-nek. Ekkor $x^p - a = x^p - \alpha^p = (x-\alpha)^p$. $x - \alpha \in L[x]$-nek pontosan egy hatványa irreducibilis: a legalacsonyabb olyan, amely $K[x]$-beli. f K fölött irreducibilisekre bontásában minden tényező azonos fokú. $\alpha \notin K$ miatt ez nem lehet $x - \alpha$, tehát p prímsége miatt $(x - \alpha)^p$. Vagyis f irreducibilis, tehát inszeparábilis. □

1.9. Galois-csoport

1.9.1. Definíció (Galois-bővítés)**.** Az $L|K$ bővítés Galois-bővítés, ha véges, normális és szeparábilis.

1.9.2. Tétel. Ha $L|K$ véges, szeparábilis bővítés, akkor egyszerű.

Bizonyítás. Ha K véges, akkor L is az, tehát a multiplikatív csoportja ciklikus. Egy generátorelemet hozzá adjungálva az egész L-et megkapjuk, tehát $L|K$ egyszerű.

Legyen K végtelen. Először belátjuk, hogy ha $K(\alpha,\beta)$ véges, szeparábilis bővítés, akkor előáll $K(\vartheta)$ alakban. Legyen α kanonikus polinomja f, β kanonikus polinomja g, fg felbontási teste M, és M-ben $f(x)=(x-\alpha_1)\cdot ...\cdot(x-\alpha_n)$ és $g(x)=(x-\beta_1)\cdot ...\cdot(x-\beta_n)$, ahol $\alpha_1=\alpha,\beta_1=\beta$.

Tekintsük az $\alpha_i+x\beta_j=\alpha+x\beta$ egyenletek $z_{ij}=\frac{\alpha-\alpha_i}{\beta_j-\beta}$ megoldásait, ahol $j\neq 1$. Mivel $L|K$ szeparábilis, $\beta_j\neq\beta$, tehát ezek értelmesek. Véges sok z_{ij} van, tehát K-nak van mindegyiktől különböző c eleme. Legyen $\vartheta=\alpha+c\beta$. Ekkor $K(\vartheta)\leq K(\alpha,\beta)$.

Tekintsük $K(\vartheta)[x]$-ben a $g(x), f(\vartheta-cx)$ polinomokat. β mindkettőnek gyöke, és mindkettő gyöktényezőkre bomlik az $M|K$ normális bővítésben. Más közös gyökük nincs, mert c választása miatt $\vartheta-c\beta_j$ nem egyenlő semelyik α_i-vel. így $\gcd(g(x),f(\vartheta-cx))=x-\beta$. Két $K(\vartheta)[x]$-beli polinom legnagyobb közös osztója is $K(\vartheta)[x]$-beli, így $\beta\in K(\vartheta)$. Ekkor $\alpha=\vartheta-c\beta\in K(\vartheta)$. Ezért $K(\alpha,\beta)=K(\vartheta)$.

Legyen L a K végtelen test véges, szeparábilis bővítése. Minden véges bővítés előáll véges sok elem adjungálásával, azaz $L=K(\alpha_1,...,\alpha_n)$. n szerinti indukcióval bizonyítunk. $n=1$-re az állítás igaz. Ha $n>1$, akkor legyen $M=K(\alpha_1,...,\alpha_{n-1})$. $M|K$ véges szeparábilis bővítés, ezért az indukciós feltétel miatt egyszerű: $M=K(\vartheta)$. Ekkor az előző bekezdés szerint $L=M(\alpha_n)=K(\vartheta,\alpha_n)$ is egyszerű. □

Speciálisan minden Galois-bővítés egyszerű.

1.9.3. Definíció (Relatív automorfizmus). A $\varphi: L\to L$ leképezés K-automorfizmusa L-nek, ha automorfizmus és K-ra megszorítva identikus.

1.9.4. Definíció (Galois-csoport). Az $L|K$ testbővítés Galois-csoportja az L test K-automorfizmusainak csoportja a kompozícióval. Jelölése $\Gamma(L|K)$.

1.9.5. Tétel. Ha $L|K$ Galois-bővítés, akkor $|\Gamma(L|K)|=(L:K)$.

Bizonyítás. $L|K$ Galois-bővítés, így egyszerű: $L=K(\alpha)$. Legyen α kanonikus polinomja f. f gyöktényezőkre bomlik L fölött. A $\varphi\in\Gamma(L|K)$ K-automorfizmust $\varphi(\alpha)$ egyértelműen meghatározza, tehát $|\Gamma(L|K)|$ annyi, ahány konjugáltja van α-nak.

$f(\alpha)=0$ miatt minden $\varphi\in\Gamma(L|K)$-ra $f(\varphi(\alpha))=\varphi(f(\alpha))=\varphi(0)=0$. Vagyis $\varphi(\alpha)$ kanonikus polinomja osztója f-nek. α és $\varphi(\alpha)$ szerepcseréjével (vagyis φ helyett φ^{-1}-et véve) $\varphi(\alpha)$ kanonikus polinomja is f. Tehát f minden konjugáltjának ugyanaz a kanonikus polinomja, mint f-nek. $\deg\alpha=\deg f=(L:K)$ miatt $|\Gamma(L|K)|\leq(L:K)$.

Már csak azt kell belátnunk, hogy f minden gyöke konjugáltja α-nak. A művelettartás felhasználásával minden $\beta \in L, f(\beta) = 0$-hoz megadható olyan $\varphi \in \Gamma(L|K)$, amelyre $\varphi(\alpha) = \beta$.

L elemeit felírjuk α, ill. β polinomjaiként, és minden $a \in L$ elemhez hozzárendeljük azt a $b \in L$ elenet, amely β-nak ugyanazon polinomjaként van felírva, mint amely polinomjaként az α-nak a. (Ekvivalensen: az elemek felírásánál az α hatványaiból álló bázisról áttérünk a β hatványaiból álló bázisra.) □

1.9.6. Definíció. Az $f \in K[x]$ polinom Galois-csoportján az f felbontási testének (mint K bővítésének) Galois-csoportját értjük. Jele $\Gamma(f)$.

1.9.7. Definíció. Legyen $L|K$ Galois-bővítés és $\Gamma = \Gamma(L|K)$.

$K \leq M \leq L$ esetén legyen $M^* = \{\varphi \in \Gamma | \forall x \in L : x^\varphi = x\}$ az L M-automorfizmusainak csoportja, vagyis $\Gamma(L|M)$.

$1 \leq H \leq \Gamma$ esetén $H^\circ = \{x \in L | \forall \varphi \in H : x^\varphi = x\}$ a H fixteste.

1.9.8. Tétel.

$$H_1 \leq H_2 \Rightarrow H_1^\circ \geq H_2^\circ$$
$$M_1 \leq M_2 \Rightarrow M_1^* \geq M_2^*$$
$$H^{\circ *} \geq H$$
$$M^{*\circ} \geq M$$

Mindegyik nyilvánvaló.

1.9.9. Tétel (A Galois-elmélet alaptétele)**.** A $* : M \to M^*$ és $\circ : H \to H^\circ$ leképezések egymás inverzei.

1.10. Véges testek

1.10.1. Tétel (Véges testek)**.** Minden p^d prímhatványra izomorfia erejéig egyértelműen létezik $q = p^d$ elemű test, és más véges test nincs. A q elemű véges test az $x^q - x \in \mathbb{F}_p[x]$ polinom $\mathbb{Z}_p$ fölötti felbontási teste. A q elemű véges testet $\mathbb{F}_q$-val jelöljük.

Bizonyítás. Ha p prím, akkor $\mathbb{Z}_p$ p elemű test, és az egyetlen ilyen, mert p karakterisztikájú és nincs valódi részteste, tehát minden p karakterisztikájú test tartalmazza. Ezt $\mathbb{F}_p$-vel jelöljük.

Minden 0 karakterisztikájú test végtelen, tehát minden véges test prím karakterisztikájú. Ha L véges test, akkor véges dimenziós vektortér $\mathbb{F}_p$ fölött valamely p prímre. Ezért az elemszáma prímhatvány.

Legyen p prím, $d > 0$ egész, és tekintsük a $\vartheta(x) = x^q - x \in \mathbb{F}_p[x]$ polinomot. Legyen K ennek egy felbontási teste. Ez véges bővítése $\mathbb{F}_p$-nek, tehát véges test. $\vartheta' \equiv -1$ miatt $\gcd(\vartheta, \vartheta') = 1$. Ezért $\vartheta(x)$ minden gyöke egyszeres.

$\varphi(x) := x^q$ testautomorfizmus, vagyis ϑ gyökei megegyeznek φ fixpontjaival. Tehát a ϑ gyökeinek a halmaza éppen a φ fixteste. De ekkor ez a fixtest azonos K-val (mert mindegyik gyököt tartalmazza), tehát K egy q elemű test.

K a ϑ felbontási teste, ezért egyértelmű. $\vartheta(x) = x(x^{q-1} - 1)$ miatt ϑ nem 0 gyökei éppen a $q - 1$-edik egységgyökök. □

2. Egységgyökök és körosztási polinomok

2.1. Egységgyökök és körosztási testek

Legyen K test és n egész.

2.1.1. Definíció (Egységgyök). $\varepsilon \in K$ n-edik egységgyök, ha $\varepsilon^n = 1 \in K$.

$\varepsilon \in K$ primitív n-edik egységgyök, ha $\varepsilon^n = 1 \in K$ és bármely $m < n$-re $\varepsilon^n \neq 1 \in K$ (vagyis $o_{K^*}(\varepsilon) = n$).

Az n-edik egységgyökök csoportot alkotnak a szorzásra.

Ha $m \mid n$, akkor minden m-edik egységgyök n-edik egységgyök is. Minden ε n-edik egységgyökhöz pontosan egy olyan $m \mid n$ van, amelyre ε primitív m-edik egységgyök.

Minden K-beli n-edik egységgyök gyöke az $x^n - 1 \in K[x]$ polinomnak, ezért K-ban legfeljebb n db n-edik egységgyök lehet. Ha az L testben van primitív n-edik egységgyök, akkor "mindegyik" (mind az n db) n-edik egységgyök benne van, vagyis $x^n - 1$ felbomlik L fölött.

Tegyük fel, hogy $x^n - 1$ felbomlik L fölött. Ebből nem következik, hogy L-ben van *primitív* n-edik egységgyök. Az L-beli n-edik egységgyökök összege a megfelelő Viète-formula alapján $x^n - 1$ $n-1$-edfokú együtthatójának az ellentettje, vagyis $n = 1$-re 1, $n > 1$-re 0.

2.1.2. Tétel. Egy test multiplikatív csoportjának minden véges részcsoportja ciklikus. Speciálisan egy véges test multiplikatív csoportja ciklikus, vagyis $\mathbb{F}_q^* \simeq Z_{q-1}$.

Bizonyítás. Legyen K test, $G \leq K^*$ véges részcsoport, és G exponense n. Ekkor $\forall a \in G : a^n = 1$, ahol 1 a K egységeleme. Tehát G minden eleme gyöke az $x^n - 1 \in K[x]$ polinomnak. Ekkor $|G| \leq n$. G kommutatív, ezért van n-edrendű eleme. Ez csak úgy lehetséges, hogy $G \simeq Z_n$, vagyis ciklikus. □

2.1.3. Definíció (Körosztási test). Az $x^n - 1 \in K[x]$ polinom K fölötti felbontási testét a K fölötti n-edik körosztási testnek nevezzük. Tehát ez a legszűkebb olyan bővítése K-nak, amelyben mind az n db n-edik egységgyök benne van.

Legyen $char(K) = p$. Ekkor $x^{p^l} - 1 = (x-1)^{p^l}$ miatt K-ban minden p-edik, sőt minden $l > 0$ egészre minden p^l-edik egységgyök 1. (Így persze a K fölötti p^l-edik körosztási test is K.)

2.1.4. Tétel. Legyen K test, n egész, és a K fölötti n-edik körosztási test L. L-ben pontosan akkor van *primitív* n-edik egységgyök, ha $char(K) \nmid n$ (vagyis $char(K) = 0$ vagy $char(K) = p$, ahol $p \nmid n$ prím).

Bizonyítás. Legyen K rögzített. A $char(K)$-val nem osztható n egészekre indukcióval látjuk be az állítást. $n = 1$-re triviális.

Tegyük fel, hogy $char(K) \nmid n$, és tudjuk, hogy minden $m \mid n, m < n$-re L-ben van *primitív* m-edik egységgyök.

Legyen $m \mid n$ és $n = km$. Ekkor

$$x^n - 1 = (x^m - 1) \cdot \sum_{j=0}^{k-1} x^{jm}$$

Legyen $\varepsilon \in L$ m-edik egységgyök. Ekkor

$$\sum_{j=0}^{k-1} \varepsilon^{jm} = \sum_{j=0}^{k-1} 1 = k \neq 0 \in K$$

mert $char(K) \nmid n = km$. Tehát az $x^m - 1$ és $\sum_{j=0}^{k-1} x^{jm}$ polinomoknak nincs közös gyöke L-ben.

Ez azt jelenti, hogy minden $m \mid n$-re az $x^n - 1$ polinom L-beli gyökei között *multiplicitással* is csak m db m-edik egységgyök van.

Az indukciós feltevés miatt minden $m \mid n, m < n$-re van primitív m-edik egységgyök L-ben, tehát $\varphi(m)$ db van.

Ezért L-ben van $\varphi(n)$ db olyan n-edik egységgyök, amely nem primitív m-edik egységgyök semmilyen $m \mid n, m < n$-re. Ezek tehát primitív n-edik egységgyökök.

Most tegyük fel, hogy $char(K) \mid n$. Ekkor $char(K) = p$ prím, és $n = p^l \cdot m$, ahol $p \nmid m$. Ekkor L-ben:

$$x^{p^l \cdot m} - 1 = (x^m - 1)^{p^l}$$

Tehát ha ε $n = p^l \cdot m$-edik egységgyök, akkor m-edik egységgyök is, vagyis nem primitív n-edik egységgyök. □

2.1.5. Tétel. Ha L-ben van primitív n-edik egységgyök, akkor L-ben a primitív n-edik egységgyökök összege $\mu(n) \in \{-1, 0, 1\} \subseteq K$.

Bizonyítás. Indukció n szerint. $n = 1$-re triviális. Tegyük fel, hogy $n > 1$, és n minden nála kisebb m osztójára igaz. Ekkor a primitív n-edik egységgyökök összege az egységgyökök összegére vonatkozó tétel és a Möbius-függvényre vonatkozó tétel miatt:

$$-\sum_{m|n}^{m<n} \mu(m) = \sum_{m|n} \mu(m) - \sum_{m|n}^{m<n} \mu(m) = \mu(n)$$

□

2.2. Körosztási polinomok

2.2.1. Definíció (Körosztási polinom)**.** Legyen K olyan test, amelyre $char(K) \nmid n$. Ekkor a K fölötti n-edik körosztási polinom az a polinom, amelynek a gyökei pontosan a K fölötti n-edik körosztási testben levő primitív n-edik egységgyökök, mindegyik egyszer. Jele: Φ_n.

Ezzel a definícióval az n-edik körosztási polinomot $\mathbb{Q}$ fölött minden n-re megadtuk, $\mathbb{F}_p$ fölött csak a p-vel nem osztható n-ekre.

2.2.2. Tétel.

$$x^n - 1 = \prod_{m|n} \Phi_m(x)$$

Bizonyítás. A körosztási polinom definíciója miatt az egyenlőség jobb oldalán $x^n - 1$ minden tényezője pontosan egyszer szerepel. □

Legyen K tetszőleges test.

2.2.3. Definíció (Körosztási polinom)**.** A K fölötti n-edik körosztási polinom n szerinti rekurzióval

$$\Phi_n(x) := \frac{x^n - 1}{\prod_{m|n}^{m<n} \Phi_m(x)}$$

Ez a definíció a fenti tétel miatt kiterjesztése az előzőnek.

2.2.4. Tétel. A körosztási polinomok egész együtthatósak. Ezért az egységgyökök algebrai egészek.

Bizonyítás. Indukció n szerint. $n = 1$-re triviális. Ha n minden nála kisebb osztójára tudjuk, akkor a fenti szorzatformulából következik n-re. □

2.2.5. Tétel. Az $\mathbb{F}_p$ fölötti Φ_n egyenlő a $\mathbb{Q}$ fölötti Φ_n-nel modulo p. Ha a $\mathbb{Q}$ fölötti Φ_n-et modulo p vesszük, akkor az $\mathbb{F}_p$ fölötti Φ_n-et kapjuk.

Bizonyítás. Tetszőleges K test fölött az n-edik körosztási polinom gyökeinek összege $\mu(n) \in \{-1, 0, 1\} \subseteq K$. Erre a 2.1.5. Tétel bizonyítása megismételhető úgy, hogy "a primitív n-edik egységgyökök összege" helyett "az n-edik körosztási polinom gyökeinek összegét" vesszük.

A körosztási polinom együtthatói: a gyökök (spec. primitív egységgyökök) előjeles elemi szimmetrikus polinomjai.

Ezeket a Newton-Girard-formulák segítségével előállítjuk a primitív egységgyökök hatványösszegeinek egész együtthatós polinomjaként. A primitív egységgyökök hatványösszegei valamilyen primitív egységgyökök összegének egész számszorosai.

Ez alapján az n-edik körosztási polinom k-adfokú együtthatójának kiszámítása nem függ az alaptesttől, csak n-től és k-tól. Az így kapott egész számot $\mathbb{Q}$ fölött változatlanul hagyjuk, $\mathbb{F}_p$ fölött pedig modulo p vesszük. □

2.2.6. Tétel. $\mathbb{F}_p$ fölött $\Phi_{p^l \cdot m} = \Phi_m^{\varphi(p^l)} = \Phi_m^{p^{l-1} \cdot (p-1)}$

Bizonyítás. A 2.1.4. Tétel bizonyításának megfelelő iránya szerint az $n = p^l \cdot m$-edik egységgyökök az m-edik egységgyökök egyenként p^l-szeres multiplicitással. □

Legyen az $x^{p^l \cdot m} - 1 \in K[x]$ polinom gyökeinek halmaza G, ez a multiplicitásoktól eltekintve azonos az $x^m - 1 \in K[x]$ polinom gyökeinek halmazával. Legyen $Z_{p^l \cdot m} \to G$ szürjektív homomorfizmus.

Legyen $\varphi : \mathbb{Z}_{q^l \cdot m} \to \mathbb{Z}_m$ homomorfizmus. Az $n = q^l \cdot m, H = H_0$ esetet $p = q$-ra úgy értelmezzük, hogy vesszük az $n = m, H = \varphi(H_0)$ esetet $p = q$-ra, majd a kapott $f_{n,H}$ polinomot p^l-edik hatványra emeljük.

Legyen $p \mid n$, $p \nmid m$ és $l \in \mathbb{Z}$. Ekkor azt mondjuk, hogy az $\mathbb{F}_p$ fölötti primitív $m \cdot p^l$-edik egységgyökök az $\mathbb{F}_p$ fölötti primitív m-edik egységgyökök egyenként $\varphi(p^l)$-szeres multiplicitással.

2.2.7. Tétel. Legyen n egész és $p \nmid n$ prím. Ekkor Φ_n pontosan akkor oldható meg modulo p, ha $p \equiv 1$ modulo n; és ekkor gyöktényezőkre is bomlik modulo p.

Bizonyítás. $p \equiv 1$ modulo $n \Leftrightarrow n \mid p - 1 = |\mathbb{F}_p^*| \Leftrightarrow \exists \varepsilon \in \mathbb{F}_p : o_{\mathbb{F}_p^*}(\varepsilon) = n \Leftrightarrow \exists \varepsilon \in \mathbb{F}_p : \Phi_n(\varepsilon) = 0$.

Ha Φ_n megoldható modulo p, akkor $\mathbb{F}_p$-ben van primitív n-edik egységgyök. De ekkor mindegyik primitív n-edik egységgyök benne van, tehát Φ_n gyöktényezőkre bomlik modulo p. □

2.2.8. Tétel. Ha $p \mid n$, akkor Φ_n nem oldható meg modulo p^2.

Bizonyítás. Feltehetjük, hogy n négyzetmentes.

Legyen $p \mid n$, és feltehetjük, hogy Φ_n megoldható modulo p.

Tegyük fel indirekt, hogy Φ_n megoldható modulo p^2, vagyis van olyan a egész, hogy $p^2 \mid \Phi_n(a) \Leftrightarrow o_{p^2}(a) = n$.

Ekkor $p \mid n$ miatt van olyan b egész, hogy $o_{p^2}(b) = p \Leftrightarrow p^2 \mid \Phi_p(b)$. Ez ekvivalens azzal, hogy $b \equiv 1$ modulo p és $b \not\equiv 1$ modulo p^2.

Ha $b \equiv 1$ modulo p^2, akkor

$$\Phi_p(b) \equiv \Phi_p(1) = \sum_{i=0}^{p-1} 1 = p$$

modulo p^2.

Ha $b \equiv 1$ modulo p és $b \not\equiv 1$ modulo p^2, akkor

$$\Phi_p(b) = \sum_{j=0}^{p-1} b^j \equiv \sum_{j=0}^{p-1} (jp+1) = p+p\cdot\sum_{j=0}^{p-1} j = p+p\cdot\frac{p(p-1)}{2} = p+\frac{p^2(p-1)}{2} \equiv p$$

modulo p^2.

Tehát $p^2 \nmid \Phi_p(b)$, ami ellentmondás. □

2.2.9. Tétel. Legyen n egész, $p \mid n$ prím, és $n = p^l \cdot m$, ahol $p \nmid m$. Ekkor Φ_n pontosan akkor oldható meg modulo p, ha $p \equiv 1$ modulo m; és ekkor gyöktényezőkre is bomlik modulo p. Tehát n-nek csak a legnagyobb prímosztója lehet ilyen.

Bizonyítás. $\mathbb{F}_p$ fölött $\Phi_{p^l \cdot m} = \Phi_m^{\varphi(p^l)} = \Phi_m^{p^{l-1}\cdot(p-1)}$

Ezért $\Phi_{p^l \cdot m}$ pontosan akkor oldható meg modulo p, ha Φ_m megoldható. Ez pontosan akkor teljesül, ha $p \equiv 1$ modulo m; és ekkor gyöktényezőkre is bomlik modulo p. □

Az n prímosztóit triviális vagy nulladik típusú kivételnek nevezzük: az ő esetükben az $f_{n,H}$ polinom $\mathbb{F}_p$ fölötti, gyökei általi megadása a fentinél kicsit technikásabb, de lehetséges. (Az együtthatói valójában ugyanazok, mint a $\mathbb{Q}$

fölötti együtthatók modulo p. De a polinom gyökeinek vizsgálatához az adott test fölötti megadás lényeges része a gyökök adott test fölötti megadása.) Ezért vannak a tételben eleve kizárva. Később velük is foglalkozunk, és meghatározzuk, hogy $p \mid n$ esetén $f_{n,H}$ mikor oldható meg modulo p.

A polinom együtthatóinak kiszámításakor a primitív n-edik egységgyökökről valójában csak azt használjuk fel, hogy az összegük $\mu(n) \in \mathbb{Z}$. A fentiek szerint $p \mid n$ esetén is megadtunk egy hasonló konstrukciót $\mathbb{F}_p$ fölött.

2.2.10. Tétel. Legyen n egész. Ekkor $D(\Phi_n)$ minden prímosztója osztja n-et.

Bizonyítás. Ha $p \nmid n$, akkor az $\mathbb{F}_p$ fölötti primitív n-edik egységgyökök (akár $\mathbb{F}_p$-beliek, akár nem) páronként különbözők (mert egy $\mathbb{Z}_n$-nel izomorf multiplikatív részcsoport generátorelemei). Ekkor $\mathbb{F}_p$ fölött $D(\Phi_n) \neq 0 \in \mathbb{F}_p$, vagyis $p \nmid D(\Phi_n) \in \mathbb{Z}$. □

2.3. Végtelen sok prím bizonyos halmazokban

2.3.1. Tétel. Legyen n egész. Ekkor végtelen sok $na + 1$ alakú prím van (vagyis olyan p prím, amelyre $p \equiv 1$ modulo n).

Bizonyítás. Feltehetjük, hogy $n > 1$. Ekkor Φ_n konstans tagja 1. Belátjuk, hogy minden N egész számhoz van olyan $na+1$ alakú prím, amely nem osztja N-et.

$\Phi_n(nN)$ relatív prím n-hez, ezért a 2.2.7. Tétel miatt $\Phi_n(nN)$ minden prímosztója $na + 1$ alakú, és egyik sem osztja N-et. (Ebből még nem következik, hogy van prímosztója!) $\Phi_n : \mathbb{R} \to \mathbb{R}$ szigorúan monoton növekvő függvény, mert a definíciójában mindegyik gyöktényező szigorúan monoton növekvő függvény. $\Phi_n(2)$ mindegyik gyöktényezője nagyobb, mint $\Phi_1(2) = 2 - 1 = 1$, tehát a szorzatuk is nagyobb.

$$\Phi_n(nN) \geq \Phi_n(2) > \Phi_1(2) = 2 - 1 = 1$$

miatt $\Phi_n(nN)$-nek van prímosztója. □

2.3.2. Tétel. Legyen p prím és l pozitív egész. Ekkor végtelen sok olyan prím van, amely $p^l \cdot a + 1$ alakú, de nem $p^{l+1} \cdot a + 1$ alakú.

(A tétel állítása $l = 0$-ra azt mondja, hogy végtelen sok nem $pa + 1$ alakú prím van. Ez $p = 2$-re nem igaz, $p > 2$-re következik az 1.1.3. Tételből ($n = p, H = \{1\}$). Ezért kell $l > 0$.)

Bizonyítás. Először legyen $p = 2$. Ekkor az állítás: végtelen sok $2^{l+1} \cdot a + 2^l + 1$ alakú prím van. Ez $l = 1$-re: végtelen sok $4k + 3$ alakú prím, következik az 1.1.3. Tételből ($n = 4, H = \{1\}$). $l = 2$-re: végtelen sok $8k + 5$ alakú prím. $4(2x + 1)^2 + 1$-nek minden prímosztója $4k + 1$ alakú, és van köztük $8k + 5$ alakú.

Legyen $l \geq 3$. $16k + 9$ alakú helyettesítési értékek helyett $32k + 18 = 2(16k + 9)$ alakúakat keresünk.

$(2x + 1)^4 + 1 \equiv 17 + 1 = 18$ modulo 32

Ennek minden prímosztója $8k + 1$ alakú, és van köztük $16k + 9$ alakú.

Most legyen $p > 2$.

$l = 1$-re egyszerű.

$p = 3$-ra: $\Phi_3(x) = x^2 + x + 1 = (x+1)^2 - x = -x$, ha $(x+1)^2 = 0$, vagyis $x \equiv 2, 5, 8$ modulo 9.

Ha $x \equiv 2, 5$ modulo 9, akkor ezeknek minden prímosztója $3k + 1$ alakú, és van köztük $9k + 4$ vagy $9k + 7$ alakú.

$l \geq 2$-re

Ha $x \equiv p^l \cdot a + 1$ modulo p^{l+1}, akkor $\exists y : \Phi_{p^l}(y) = x$.

Miért van a polinomnak olyan helyettesítési értéke, amely a részcsoporton kívül van?

Innen kezdve: adott részcsoporton kívüli prím.

□

3. Másodfokú polinomok és a kvadratikus reciprocitás tétele

3.0.1. Definíció (Legendre-szimbólum). Legyen p páratlan prím és $a \in \mathbb{Z}$ (nem feltétlenül pozitív) egész. Ekkor az $\left(\frac{a}{p}\right)$ Legendre-szimbólumot a következőképpen definiáljuk: $\left(\frac{a}{p}\right)$ az az egész szám, amelyre

$$|\left(\frac{a}{p}\right)| = 1$$

és

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$$

3.0.2. Tétel (Kvadratikus reciprocitás tétele). Ha p, q páratlan prímek, akkor

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

3.0.3. Tétel (Kiegészítő lemmák). Ha p páratlan prím, akkor

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

A -1-re vonatkozó egyenlőség bizonyítása.

$$\left(\frac{-1}{p}\right) = 1 \Leftrightarrow \exists \varepsilon \in \mathbb{F}_p : \varepsilon^2 = -1$$

$$\varepsilon^2 = -1 \Leftrightarrow \varepsilon^2 + 1 = 0 \Leftrightarrow \Phi_4(\varepsilon) = 0 \Leftrightarrow o(\varepsilon) = 4$$

$\exists \varepsilon \in \mathbb{F}_p : \Phi_4(\varepsilon) = 0$, vagyis $\Phi_4 \mod p$ megoldhatósága a 2.2.7. Tételt $n = 4$-re használva ekvivalens azzal, hogy $p \equiv 1 \mod 4$. □

4. Egy általánosabb reciprocitási tétel

4.1. Bevezetés

4.1.1. Tétel (Reciprocitási tétel). Legyen $n \in \mathbb{Z}_+$, $H \leq \mathbb{Z}_n^*, |\mathbb{Z}_n^* : H| = d$ és $p \nmid n$ prím. Ekkor van olyan, $f = f_{n,H} \in \mathbb{Z}[x]$ $\mathbb{Z}$ fölött irreducibilis d-edfokú normált polinom, amelynek véges sok kivétellel pontosan akkor van gyöke modulo p, ha $p \in H$ modulo n; pontosabban minden $p \in H$ modulo n esetén gyöktényezőkre bomlik modulo p, és ezeken kívül csak véges sok p esetén van gyöke modulo p.

Tekintsük azon $m \in \mathbb{Z}_+, m \mid n$ számokat, amelyekre H előáll egy $K \leq \mathbb{Z}_m^*$ részcsoport teljes inverz képeként az egyértelműen létező $\varphi : \mathbb{Z}_n \to \mathbb{Z}_m$ homomorfizmusnál, vagyis $H = \varphi^{-1}(K)$. Jelöljük a legkisebb ilyen m-et M-mel. Ekkor m pontosan akkor ilyen, ha $M \mid m \mid n$.

Ha m ilyen, akkor $p \in H$ modulo n pontosan akkor, ha $p \in \varphi(H)$ modulo m és $p \nmid n/m$. Tehát H és K mint maradékosztályok uniója véges sok kivétellel ugyanazon prímeket tartalmazza. Elég azon H részcsoportokkal foglalkozni, amelyekre $M = n$. Ezért a továbbiakban (egyelőre) feltesszük, hogy $M = n$. Ezt úgy is mondhatjuk, hogy H csak triviálisan áll elő teljes inverz képként egy *gyűrű* homomorfizmusnál.

4.1.1. A polinom megadása a gyökei által

Adott n és H esetén a gyökei által megadunk egy megfelelő polinomot. Legyen K olyan prímtest, amelyet lehet n-edik egységgyökökkel bővíteni (beleértve azt az esetet is, hogy eleve benne vannak). (Vagyis $K = \mathbb{Q}$ vagy $K = \mathbb{F}_p$, ill. $char(K) = 0$ vagy $char(K) = p$, ahol $p \nmid n$.)

Legyen L az n-edik körosztási polinom felbontási teste K fölött, és legyen $\varepsilon \in L$ primitív n-edik egységgyök.

Ha $k \in \mathbb{Z}_n^*$ és ε primitív n-edik egységgyök, akkor ε^k is primitív n-edik egységgyök. Tehát a $\mathbb{Z}_n^*$ hat a primitív n-edik egységgyökök halmazán, és ez a hatás izomorf a $\mathbb{Z}_n^*$ reguláris permutációreprezentációjával. Ezt a hatást megszorítjuk H-ra, és a primitív n-edik egységgyökök ezen megszorítás szerinti orbitjait a primitív n-edik egységgyökök H szerinti orbitjainak (vagy röviden a H orbitjainak) nevezzük.

Ezen orbitokban minden primitív n-edik egységgyököt ε hatványaként írunk fel. Ekkor minden orbithoz a benne szereplő kitevők halmaza azonos $\mathbb{Z}_n^*$ egy H szerinti mellékosztályával modulo n. Legyen $|H| = g$, $H = \{h_1, ..., h_g\}$,

és $R = \{r_1, ..., r_d\}$ H szerinti reprezentánsrendszer $\mathbb{Z}_n^*$-ban. Ekkor a $\mathbb{Z}_n^*$ H szerinti mellékosztályai $r_1H, ..., r_dH$.

Legyenek a $\mathbb{Z}_n^*$ H szerinti mellékosztályai H_j, a primitív n-edik egységgyökök H szerinti orbitjai $\phi(H_j) = o_j$, ahol $j = 1, ..., d$.

Ekkor

$$f_{n,H}(x) = \prod_{j=1}^{d}(x - \sum_{l=1}^{g} \varepsilon^{r_j h_l})$$

egy megfelelő polinom. Tehát a gyökök bijekcióban állnak az orbitokkal, ezért $\deg f_{n,H} = |\mathbb{Z}_n^* : H| = d$.

Ezt a polinomot $f_{n,H}$-val vagy röviden f-fel jelöljük.

A konstrukció miatt a polinom gyökeinek összege $\mu(n)$.

4.1.2. Kitüntetett esetek

Ha $H = \mathbb{Z}_n^*$, akkor $f_{n,H}$ elsőfokú, egyetlen gyöke $\mu(n)$. Ekkor f minden p prímre megoldható modulo p (az n prímosztóit is beleértve), nincs kivétel.

Ha $H = 1$ a triviális részcsoport, akkor a gyökök a primitív n-edik egységgyökök, és $f_{n,H} = \Phi_n$ az n-edik körosztási polinom. Ekkor a körosztási polinomról szóló szakasz szerint az egyetlen lehetséges kivétel n legnagyobb prímosztója.

4.1.3. A polinom egész együtthatós és irreducibilis az egészek fölött

4.1.2. Tétel. Az $f_{n,H}$ polinom egész együtthatós.

Bizonyítás. Ebben a rövid bizonyításban felhasználjuk, hogy a körosztási polinomok egész együtthatósak.

f együtthatói a gyökök előjeles szimmetrikus polinomjai, ezért a $K(\epsilon) : K$ testbővítés minden automorfizmusa önmagukba viszi őket. Ezért K-beliek. Ezzel $K = \mathbb{F}_p$ esetén készen vagyunk, $K = \mathbb{Q}$ esetén csak a racionalitást tudjuk.

f gyökei egységgyökök összegei, ezért algebrai egészek. Tehát a $\mathbb{Q}$ fölötti normált minimálpolinomjuk egész együtthatós, és d-edfokú. f is d-edfokú, és osztható a minimálpolinommal, ezért konstansszorosa a minimálpolinomnak. De mivel normált, ezért egyenlő vele. Tehát f $\mathbb{Q}$ fölött is egész együtthatós. □

Az $f_{n,H}$ polinom irreducibilis $\mathbb{Q}$ fölött, mert $\mathbb{Q}$ fölötti minimálpolinomja a gyökeinek.

4.1.4. A polinom igazzá teszi a reciprocitási tételt

Az orbitokon belül a H részcsoport hat; az orbitok között, és így az f polinom gyökein a $\mathbb{Z}_n^*/H$ faktorcsoport hat.

$K = \mathbb{Q}$ esetén ez az f polinom, ill. az f K fölötti felbontási testének Galois-csoportja, és ez egy természetes reprezentációja. ($K = \mathbb{F}_p$ esetén a Galois-csoport ennek egy faktorcsoportja, de általában nem azonos vele.)

Az általánosabb reciprocitási tétel bizonyítása. Belátjuk, hogy az $f_{n,H}$ polinom helyettesítési értékeinek prímosztóira igaz a reciprocitási tételben megfogalmazott ekvivalencia.

Legyen $p \nmid n$ prím és $K = \mathbb{F}_p$. Tekintsük az f polinom gyökeit $\mathbb{F}_p$ fölött.

Tegyük fel, hogy $p \in H$ modulo n. Ekkor a p-vel való modulo n szorzás a H szerinti mellékosztályokat önmagukba viszi, a p-edik hatványozás (vagyis a Frobenius-automorfizmus) a H orbitjait önmagukba viszi, tehát f gyökeit fixálja. Ez azt jelenti, hogy f minden gyöke $\mathbb{F}_p$-beli, vagyis gyöktényezőkre bomlik $\mathbb{F}_p$-ben.

Tegyük fel, hogy $f_{n,H}$-nak van gyöke $\mathbb{F}_p$-ben.

Legyen az f $\mathbb{Q}$ fölötti felbontási teste L. Az $L|\mathbb{Q}$ bővítés normális, ill. véges és szeparábilis, tehát egyszerű. Az egyszerűség miatt ha ξ gyöke f-nek, akkor $1, \xi, ..., \xi^{d-1}$ $\mathbb{Q}$ fölötti bázisa L-nek. Ezért f bármelyik gyöke előáll bármelyik gyök *racionális* együtthatós polinomjaként. De itt az együtthatók nem feltétlenül *egészek*.

Ha a p prím ezen *racionális* együtthatós polinom semelyik együtthatójának a nevezőjét sem osztja, akkor $\mathbb{F}_p$-ben az osztások elvégezhetők. így ha az egyik gyök $\mathbb{F}_p$-beli, akkor mindegyik gyök $\mathbb{F}_p$-beli, vagyis $f_{n,H}$ gyöktényezőkre bomlik $\mathbb{F}_p$-ben.

A gyökök egymással való felírásához használt racionális együtthatós polinomok véges sokan vannak, tehát véges sok prím osztja valamelyik együttható nevezőjét. Ezért $f_{n,H}$ véges sok kivétellel gyöktényezőkre bomlik $\mathbb{F}_p$-ben.

Tegyük fel, hogy $f_{n,H}$ gyöktényezőkre bomlik $\mathbb{F}_p$-ben. Ha $D(f_{n,H}) \neq 0 \in \mathbb{F}_p$, akkor $\mathbb{F}_p$-ben $f_{n,H}$ minden gyöke egyszeres. Ekkor a Frobenius-automorfizmus a gyököket definiáló összegeket önmagukba viszi. Ezért $p \in H \mod n$.

Tehát ha a p prímre $p \notin H \mod n$, de $f_{n,H}$ gyöktényezőkre bomlik $\mod p$, akkor $f_{n,H}$ $\mathbb{F}_p$-beli gyökei közül valamelyiket több különböző összeg is megadja. Ez tehát többszörös gyök. Ekkor $D(f_{n,H}) = 0 \in \mathbb{F}_p$, vagyis $p \mid D(f_{n,H})$. Ez szintén véges sok kivételes prím. Ezért véges sok kivétellel $p \in H \mod n$.

Ezzel a tételt bizonyítottuk. □

4.2. A polinom (együtthatóinak) kiszámítása

A polinom együtthatóit felírjuk a Möbius-függvény értékeinek egész együtthatós lineáris kombinációjaként. Ez egyben egy másik bizonyítása annak, hogy a polinom egész együtthatós.

Legyen $k = 0, ..., d$, és jelölje $\sigma_k(x_1, ..., x_n)$ az $x_1, ..., x_n$ változók k-adik elemi szimmetrikus polinomját. Ekkor a $d-k$-adik együttható kiszámítása:

$$f_{n,H}[x^{d-k}] = \sigma_k(-\sum_{l=1}^{g} \varepsilon^{r_j h_l} : j = 1, ..., d) = (-1)^k \cdot \sigma_k(\sum_{l=1}^{g} \varepsilon^{r_j h_l} : j = 1, ..., d) =$$

$$= (-1)^k \cdot \sum_{j_1=1,...,j_k=k}^{d-k+1,...,d} \prod_{?=1}^{k} \sum_{l=1}^{g} \varepsilon^{r_{j_?} h_l} = (-1)^k \cdot \sum_{j_1=1,...,j_k=k}^{d-k+1,...,d} \sum_{l_1,...,l_k=1}^{g} \prod_{?=1}^{k} \varepsilon^{r_{j_?} h_{l_?}} =$$

$$= (-1)^k \cdot \sum_{j_1=1,...,j_k=k}^{d-k+1,...,d} \sum_{l_1,...,l_k=1}^{g} \varepsilon^{\sum_{?=1}^{k} r_{j_?} h_{l_?}}$$

A gyökök g tagú összegek, ezért a gyökök k tényezős szorzatai kifejtve, de nem összevonva g^k tagú összegek. Tehát a gyökök k-adik elemi szimmetrikus polinomja tagjainak száma kifejtve, de nem összevonva:

$$\binom{d}{k} \cdot g^k = \binom{d}{k} \cdot (\frac{\varphi(n)}{d})^k$$

A számolás során minden n-edik egységgyököt ε hatványaként írtunk fel, és a $0, 1, ..., n-1$ kitevőket azonosítjuk a $\mathbb{Z}_n$ gyűrű elemeivel, az ε hatványitevőit modulo n értjük. Azt kell vizsgálnunk, hogy a $\mathbb{Z}_n$ gyűrű adott eleme hányféleképpen áll elő $\mathbb{Z}_n^*$ k db különböző H szerinti mellékosztálya egy-egy elemének összegeként, vagyis $\sum_{?=1}^{k} r_{j_?} h_{l_?}$ alakban modulo n, ahol $j_1, ..., j_k$ végigfut $\{1, ..., d\}$ minden k elemű részhalmazán, és $l_1, ..., l_k$ végigfut minden $\{1, ..., g\}$ elemeiből álló rendezett k-ason.

4.2.1. Tétel. A fenti összegfelbontások száma csak az elem additív rendjétől függ.

Bizonyítás. Legyen $a, b \in \mathbb{Z}_n$ két különböző, de azonos additív rendű elem, és $o := o(a) = o(b)$. Ekkor $a \cdot c = b$ esetén $c \in \mathbb{Z}_n^*$. Az ilyen c-k száma $\varphi(n)/o$. Legyenek ezek $c_1, ..., c_{\varphi(n)/o}$. A $\sum_{?=1}^{k} r_{j_?} h_{l_?}$ formális összegek között tekintsük azt az ekvivalencia-relációt, hogy az egyik összeg a másiknak az a-szorosa, ahol $a \in \mathbb{Z}_n^*$. a egyértelműen előáll $r_j h_l$ alakban, így az a-val szorzás

Ekkor minden ekvivalenciaosztály $\varphi(n)$ elemű.

Ekkor ha egy összeg additív rendje m, akkor az ekvivalenciaosztálya m elemű. □

Legyen minden $k = 0, 1, ..., d$ egészre és minden $m \mid n$ pozitív egészre az $f_{n,H}$ gyökeinek k-adik elemi szimmetrikus polinomjában a $\mathbb{Z}_n$ gyűrű m additív rendű elemei előfordulásainak a száma (egyenként) $N_{n,H}(k, m)$ vagy röviden $N(k, m)$.

Adott k-ra az $N_{n,H}(k, m)$ számok megfelelően (a φ-függvénnyel) súlyozott összege a $d - k$-adik együtthatót kifejező összeg tagjainak a száma kifejtve, de nem összevonva:

$$\sum_{m|n} \varphi(m) \cdot N_{n,H}(k, m) = \binom{d}{k} \cdot g^k = \binom{d}{k} \cdot (\frac{\varphi(n)}{d})^k$$

Az $f_{n,H}$ polinom $d - k$-adik együtthatója:

$$f_{n,H}[x^{d-k}] = (-1)^k \cdot \sum_{m|n} \mu(m) \cdot N_{n,H}(k, m) = (-1)^k \cdot \sum_{m|rad(n)} \mu(m) \cdot N_{n,H}(k, m)$$

Speciálisan a $d - 1$-edik együttható: $f_{n,H}[x^{d-1}] = -\mu(n)$.

Ha $n = q$ prím, akkor ezek az egyenlőségek jelentősen leegyszerűsödnek.

$$(q-1) \cdot N_{q,H}(k, q) + N_{q,H}(k, 1) = \binom{d}{k} \cdot (\frac{q-1}{d})^k$$

$$f_{q,H}[x^{d-k}] = (-1)^k \cdot (N_{q,H}(k, 1) - N_{q,H}(k, q))$$

$k = 2$ esetén tovább egyszerűsödnek:

$$(q-1) \cdot N_{q,H}(2, q) + N_{q,H}(2, 1) = \binom{d}{2} \cdot (\frac{q-1}{d})^2 = \frac{d(d-1)}{2} \cdot (\frac{q-1}{d})^2$$

$$f_{q,H}[x^{d-2}] = N_{q,H}(2,1) - N_{q,H}(2,q)$$

$d = 2$ esetén tovább egyszerűsödnek:

$$(q-1) \cdot N_{q,H}(2,q) + N_{q,H}(2,1) = (\frac{q-1}{2})^2 = \frac{(q-1)^2}{4}$$

$$(q-1) \cdot N_{q,H}(2,q) = \frac{(q-1)^2}{4} - N_{q,H}(2,1)$$

$$N_{q,H}(2,q) = \frac{q-1}{4} - \frac{N_{q,H}(2,1)}{q-1}$$

$$f_{q,H}[x^0] = N_{q,H}(2,1) - N_{q,H}(2,q) = N_{q,H}(2,1) - (\frac{q-1}{4} - \frac{N_{q,H}(2,1)}{q-1}) =$$

$$= N_{q,H}(2,1) - \frac{q-1}{4} + \frac{N_{q,H}(2,1)}{q-1} = \frac{q}{q-1} \cdot N_{q,H}(2,1) - \frac{q-1}{4}$$

4.2.2. Tétel. $N_{n,H}(2,1) = 0$, ha $-1 \in H$ modulo n; és $N_{n,H}(2,1) = \frac{\varphi(n)}{2}$, ha $-1 \notin H$ modulo n.

Speciálisan, ha $n = q$ páratlan prím és H a nem 0 kvadratikus maradékok csoportja modulo q, akkor:

$N_{q,H}(2,1) = 0$, ha $-1 \in H$ modulo q, vagyis $q \equiv 1$ modulo 4; és $N_{q,H}(2,1) = \frac{q-1}{2}$, ha $-1 \notin H$ modulo n, vagyis $q \equiv -1$ modulo 4.

Bizonyítás. $N_{n,H}(2,1)$ azon 2 tagú összegek száma, amelyek értéke egy rögzített 1 additív rendű elem, vagyis 0.

A 0 pontosan akkor áll elő 2 tagú összegként, ha van olyan $a \in \mathbb{Z}_n^*$, amelyre a és $-a$ közül pontosan az egyik H-beli, vagyis ha $-1 \notin H$ modulo n. Ekkor minden $a \in \mathbb{Z}_n^*$ esetén az $(a, -a)$ rendezetlen párhoz tartozik egy összeg, ez összesen $\frac{\varphi(n)}{2}$ összeg. □

4.2.3. Tétel. Ha $n = q$ páratlan prím és $d = 2$, vagyis H a nem 0 kvadratikus maradékok csoportja modulo q, akkor a polinom:

$$f_{n,H} = x^2 + x + \frac{1 - (-1)^{\frac{q-1}{2}} \cdot q}{4} = x^2 + x + \frac{1 + (-1)^{\frac{q+1}{2}} \cdot q}{4}$$

Bizonyítás. Az elsőfokú együttható $-\mu(q) = 1$. A konstans tag:

$$f_{q,H}[x^0] = \frac{q}{q-1} \cdot N_{q,H}(2,1) - \frac{q-1}{4}$$

$q \equiv 1$ modulo 4 esetén:

$$f_{q,H}[x^0] = \frac{q}{q-1} \cdot 0 - \frac{q-1}{4} = 0 - \frac{q-1}{4} = -\frac{q-1}{4} = \frac{1-q}{4}$$

$q \equiv -1$ modulo 4 esetén:

$$f_{q,H}[x^0] = \frac{q}{q-1} \cdot \frac{q-1}{2} - \frac{q-1}{4} = \frac{q}{2} - \frac{q-1}{4} = \frac{q+1}{4} = \frac{1+q}{4}$$

□

4.3. A kvadratikus reciprocitás tételének a bizonyítása

Ha $d = 2$, vagyis f másodfokú, akkor a két gyök összege $\mu(n)$, tehát kifejezhetők egymás *egész* együtthatós polinomjaként. Ez azt jelenti, hogy minden kivételes prím osztója a polinom diszkriminánsának.

A -1-re vonatkozó kiegészítő lemmát az $n = 4, H = \{1\}$ esetre és az $f_{n,H} = \Phi_4$ körosztási polinomra hivatkozva beláttuk. A 2-re vonatkozó kiegészítő lemma kétféle bizonyítása (primál és duál):

Rövidebb bizonyítás. Legyen $n = 8, H = \{\pm 1\}$. Ekkor $f_{n,H} = x^2 - 2$. Tehát $= 1$ pontosan akkor, ha $f_{8,\{\pm 1\}} = x^2 - 2$ megoldható $\mod p$, vagyis pontosan akkor, ha $p \in H \mod n$, vagyis $p \equiv \pm 1 \mod 8$. □

Hosszabb bizonyítás. Legyen $n = q$ páratlan prím, H a $\mod q$ nem 0 kvadratikus maradékok csoportja. Ekkor

$$f_{n,H} = x^2 + x - \frac{1 - (-1)^{\frac{q-1}{2}} \cdot q}{4}$$

Ekkor $= 1$ a fenti általános reciprocitási tétel miatt pontosan akkor teljesül, ha $2 \in H \mod q$, vagyis $f_{n,H}$ megoldható $\mod 2$. $x^2 + x$ mindig páros, tehát

$$f_{n,H} \equiv \frac{1 - (-1)^{\frac{q-1}{2}} \cdot q}{4}$$

Ezért $f_{n,H}$ pontosan akkor oldható meg $\mod 2$, ha a polinom konstans tagja páros:

$$2 \mid \frac{1-(-1)^{\frac{q-1}{2}} \cdot q}{4} \Leftrightarrow 8 \mid 1-(-1)^{\frac{q-1}{2}} \cdot q$$

Ez pedig pontosan akkor teljesül, ha $q \equiv \pm 1 \mod 8$. □

A kvadratikus reciprocitás tételének bizonyítása. Az előző tételben szereplő polinom diszkriminánsa:

$$D = 1-4\cdot\frac{1-(-1)^{\frac{q-1}{2}} \cdot q}{4} = 1-(1-(-1)^{\frac{q-1}{2}}\cdot q) = 1-1+(-1)^{\frac{q-1}{2}}\cdot q = (-1)^{\frac{q-1}{2}}\cdot q$$

□

4.4. A kivételes prímek vizsgálata

Ha a p prímre ($p \nmid n$ és) $p \notin H$ modulo n, de $f_{n,H}$-nak van gyöke $\mod p$, akkor p-t (valódi) kivételes prímnek vagy kivételnek nevezzük. (Ezen belül még meg fogunk különböztetni két típust. Egy valódi kivételnek minősített prímről később kiderülhet, hogy mégsem az, ill. kiderülhet, hogy $p|n$, vagyis triviális kivétel.)

Ha a p prím ezen *racionális* együtthatós polinom valamelyik együtthatójának a nevezőjét osztja, akkor $\mathbb{F}_p$-ben 0-val kellene osztani.

$$\xi = \sum_{j=0}^{d} a_j \cdot \xi_1^j$$

ahol $(a_j \in \mathbb{Q})$. Legyen az együtthatók nevezőjében a p hatványkitevőinek maximuma $l > 0$. Szorozzuk meg ezt a polinom-előállítást p^l-lel (így minden nevezőből eltűnik a p, de marad nem 0 tag). Ha ezt modulo p nézzük, ebben már nem is szerepel ξ, és így azt jelenti, hogy ϵ gyöke egy bizonyos polinomnak modulo p. Ez azt jelenti, hogy ha az eredeti polinom tagjait közös nevezőre hozzuk (ill. elég a nevezők pontos p-hatvány osztóját közössé tenni), akkor a számláló is 0. Tehát a formula ξ-re nézve nem ellentmondásos, hanem tautologikus.

Így ha az egyik gyök $\mathbb{F}_p$-beli, akkor ebből semmi nem következik a többi gyökre. (Tehát lehet, hogy valamelyik gyök nem $\mathbb{F}_p$-beli; ill. lehet, hogy mégis mindegyik gyök $\mathbb{F}_p$-beli.) Ezeket a prímeket első típusú kivételnek nevezzük.

Tegyük fel, hogy p nem első típusú kivétel, és így mindegyik gyök $\mathbb{F}_p$-beli. Ekkor indirekt feltesszük, hogy $p \notin H$. Ekkor a Frobenius-endomorfizmus a H orbitjait nem önmagukba viszi. A Frobenius-endomorfizmus rendje annyi, amennyi a pH elem rendje a $\mathbb{Z}_n^*/H$ faktorcsoportban, és a H orbitjait ekkora osztályokban permutálja egymásba. Tehát a gyökök ekkora osztályokban azonosak. Vagyis mindegyik gyök multiplicitása osztható ezzel a számmal. Ez csak akkor lehetséges, ha p osztója $D(f)$-nek. Ezeket a prímeket második típusú kivételnek nevezzük. Ilyenről is kiderülhet, hogy valójában nem kivétel.

Egy első vagy második típusú kivételről kiderülhet, hogy osztója n-nek. Ez ellentmond a kezdeti feltevésünknek, és ekkor triviális kivétel.

4.4.1. Tétel. Ha $p = d \in H$ modulo n, akkor $p \mid (f_{n,H})[x^0] \cdot D(f_{n,H})$.

Bizonyítás. Ha $p = d \in H$ modulo n, akkor $f_{n,H}$ gyöktényezőkre bomlik modulo p. Tehát $d = p$ db gyöke van $\mathbb{F}_p$-ben. Ha $f_{n,H}$-nak gyöke $0 \in \mathbb{F}_p$, akkor $p \mid (f_{n,H})[x^0]$. Ha nem gyöke, akkor $p - 1 < d$ és a skatulyaelv miatt van többszörös gyöke. Ekkor $D(f_{n,H}) = 0 \in \mathbb{F}_p$, vagyis $p \mid D(f_{n,H})$. □

4.4.2. Tétel. Ha $p \in H$ modulo n és $p < d$, akkor $p \mid D(f_{n,H})$.

Bizonyítás. Ha $p \in H$ modulo n, akkor $f_{n,H}$ gyöktényezőkre bomlik modulo p. Tehát d db gyöke van $\mathbb{F}_p$-ben. Így $p < d$ és a skatulyaelv miatt van többszörös gyöke. Ekkor $D(f_{n,H}) = 0 \in \mathbb{F}_p$, vagyis $p \mid D(f_{n,H})$. □

A valódi (n-et nem osztó) kivételes prímek létezése egy olyan lehetőség, amelyet a téma vizsgálatakor figyelembe kell venni, mert nem zárható ki triviálisan. Viszont jelenleg egyetlen valódi kivételt sem ismerek. Lehet, hogy nincs is valódi kivétel.

Hivatkozások

[1] David A. Cox, *Primes of the form* $x^2 + ny^2$, Wiley, New York, 1989.

[2] Kiss Emil, *Bevezetés az algebrába*, Typotex, Budapest, 2007.

[3] Pelikán József, Gröller Ákos, *Algebra*, Budapest, 2000