Universiteit Utrecht

Bachelorscriptie

# Gauss-sommen over algebra's

*Auteur:*
B.J. Ringeling
4123468

*Begeleider:*
Prof. Dr. F. Beukers

7 juni 2016

# Inhoudsopgave

# Hoofdstuk 1

# Inleiding

Gauss-sommen zijn eindige sommen van eenheidswortels. Oorspronkelijk werden deze sommen onderzocht door C.F. Gauss, die in eerste instantie keek naar de som $\sum_{n=0}^{p-1} e^{\frac{2\pi i n^2}{p}}$. Gauss vond de volgende waarden bij deze som: $\sqrt{p}$ als $p \equiv 1 \ mod \ 4$ en $i\sqrt{p}$ als $p \equiv 3 \ mod \ 4$. In het algemeen blijkt het berekenen van het argument (de hoek van de Gauss-som in het complexe vlak) van de Gauss-som een erg zware opgave te zijn en hier is ook nog geen algemene uitdrukking voor. De modulus van de Gauss-som is echter wat eenvoudiger om te bekijken. Op enkele uitzonderingen na blijkt de modulus, bij eindige lichamen, gelijk te zijn aan de wortel van de kardinaliteit van dat lichaam. In deze scriptie wordt onderzocht in welke mate de stellingen over Gauss-sommen op eindige lichamen waar blijven in algemene algebra's over deze eindige lichamen.
Eerst zal er een introductie worden gegeven over Gauss-sommen op eindige lichamen, waarin enkele elementaire eigenschappen worden bewezen. In de daarop volgende hoofdstukken zal gezocht worden naar additieve karakters op algemene algebra's over een eindig lichaam.
In hoofdstuk 3 zullen de Gauss-sommen op de algebra's $\mathbb{F}_q[X]/(f(X))$ worden onderzocht, waar $f(X)$ een separabel polynoom is. Dit blijkt een relatief eenvoudige analyse te zijn, omdat we de additieve karakters voor eindige lichamen direct kunnen gebruiken om de Gauss-sommen op dit type algebra's te bekijken.
In hoofdstuk 4 zal worden gekeken naar algebra's van de vorm $\mathbb{F}_q[X]/(f(X))$, waar $f(X)$ een inseparabel polynoom is. Het bleek lastig om de analogie voor eindige lichamen te gebruiken om Gauss-sommen hierop te bekijken. Er wordt in dit hoofdstuk een expliciete uitdrukking gegeven van de modulus van de Gauss-som op deze algebra's. De modulus op deze algebra's zal vergelijkbaar zijn met de modulus bij eindige lichamen.
Uiteindelijk zal de Gauss-som $\mathbb{F}_p[X]/(X^n)$ concreet worden berekend in hoofdstuk 5. Dit zal voor enkele $n$ worden gedaan, waarbij gebruik gemaakt wordt van kwadratische Gauss-sommen.

# Hoofdstuk 2

# Gauss-sommen op eindige lichamen

## 2.1 Karakters op eindige groepen

Voordat Gauss-sommen gedefinieerd kunnen worden, is eerst het begrip "karakter" op eindige groepen van belang.

**Definitie 2.1.1.** Laat G een eindige abelse groep zijn. Een karakter $\chi$ op G is een groepshomomorfisme naar de multiplicatieve groep $\mathbb{C}^*$.

Omdat G een eindige groep is, is elk element van eindige orde. Hieruit volgt dat ieder karakter een complexe eenheidswortel is. Als $G$ cyclisch is met generator $g$, dan wordt $\chi$ volledig bepaald door $\chi(g)$. Immers, voor elk element $a$ uit de groep $G$ geldt $\chi(a) = \chi(g^k) = \chi(g)^k$. Dit geeft dus in dat geval precies $|G|$ mogelijke karakters.

**Definitie 2.1.2.** Een karakter $\chi$ heet triviaal als $\chi(a) = 1$ voor elke a in G. We schrijven $\chi = \varepsilon$.

Het is eenvoudig na te gaan dat het triviale karakter inderdaad een karakter is. Eerst leiden we wat algemene eigenschappen van karakters af met de volgende propositie.

**Propositie 2.1.1.** *Als $\chi$ een karakter is op een groep $G$ en $a \in G$, dan geldt het volgende:*

*(i)* $\chi(e) = 1$ *(e is de eenheid van G)*

*(ii)* $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$

*Bewijs.* (i) Dit is vrij eenvoudig in te zien, immers: $\chi(e) = \chi(e \cdot e) = \chi(e) \cdot \chi(e)$ dus $\chi(e) = 1$ omdat $\chi(e) \neq 0$. (ii) Uit (i) volgt dat $1 = \chi(e) = \chi(a \cdot a^{-1}) = \chi(a) \cdot \chi(a^{-1})$. Dit laat zien dat $\chi(a^{-1}) = \chi(a)^{-1}$. Het rechter gedeelte van de gelijkheid volgt uit het feit dat $\chi(a)$ op de complexe eenheidscirkel ligt. □

Voor de analyse van Gauss-sommen blijkt het volgende (simpele) lemma van belang.

**Propositie 2.1.2.** *Laat $\chi \neq \varepsilon$ een karakter zijn op $G$ en laat $S = \sum_{a \in G} \chi(a)$. Dan volgt $S = 0$ als $\chi \neq \varepsilon$, anders volgt $S = |G|$.*

*Bewijs.* De laatste bewering is voor de hand liggend. Stel nu $\chi \neq \varepsilon$, dan volgt dat er een $b \in G$ bestaat zodat $\chi(b) \neq 1$. Dit betekent dat $\chi(b)S = \sum_{a \in G} \chi(ab) = S$. Immers, er is een bijectie $a \to ab$. Omdat geldt dat $\chi(b) \neq 1$ volgt dat $S = 0$. □

De verzameling van karakters op een eindige abelse groep $G$ vormt zelf ook weer een groep $\widehat{G}$, met als groepsoperatie de puntsgewijze vermenigvuldiging van de karakters en als eenheid het triviale karakter. Het is eenvoudig na te gaan dat dit inderdaad een groep vormt. Er blijkt te gelden dat $|\widehat{G}| = |G|$. Om dit te laten zien hebben we de zogenaamde structuurstelling nodig voor eindige abelse groepen.

**Stelling 2.1.3** ([3], 2.1.9)**.** *Laat $G$ een eindige abelse groep zijn. Dan bestaan er unieke gehele getallen $m_i > 1$ met $1 \leq i \leq k$ en $m_i | m_{i+1}$ voor elke $1 \leq i < k$, zodat*

$$G \simeq \bigoplus_{i=1}^{k} (\mathbb{Z}/m_i\mathbb{Z})$$

*Bewijs.* Zie ([3], 2.1.9). □

**Propositie 2.1.4** ([3], 2.1.16)**.** *Laat $G$ een eindige abelse groep zijn. Dan geldt $|\widehat{G}| = |G|$.*

*Bewijs.* Met behulp van de vorige stelling weten we dat $G \simeq \bigoplus_{i=1}^{k} (\mathbb{Z}/m_i\mathbb{Z})$. Verder is eenvoudig in te zien dat $\widehat{G_1 \oplus G_2} \simeq \widehat{G_1} \oplus \widehat{G_2}$. Er hoeft dus nog alleen bewezen te worden dat $|\widehat{(\mathbb{Z}/m_i\mathbb{Z})}| = |(\mathbb{Z}/m_i\mathbb{Z})|$. Dit laatste volgt uit het feit dat $(\mathbb{Z}/m_i\mathbb{Z})$ een cyclische groep is met als generator 1. Elke karakterwaarde op $(\mathbb{Z}/m_i\mathbb{Z})$ wordt volledig bepaald door de karakterwaarde op 1, immers $\chi(g) = \chi(1)^g$. De karakterwaarde op 1 kan gekozen worden als willekeurige $m$-e machts eenheidswortel. Er volgt nu dus $|(\mathbb{Z}/m_i\mathbb{Z})| = (\mathbb{Z}/\hat{m}_i\mathbb{Z})$ en hierbij is dus bewezen dat $|\widehat{G}| = |G|$. □

**Definitie 2.1.3.** Laat A een ring zijn. $\chi$ heet een multiplicatief karakter als $\chi$ een karakter is op de eenhedengroep $A^*$. $\chi$ heet een additief karakter als $\chi$ een karakter is op de optellingsgroep $A^+$.

**Voorbeeld**. Het Legendresymbool $\left(\frac{\cdot}{p}\right)$ op $\mathbb{F}_p^*$ is een karakter van orde twee. Omdat het Legendresymbool een multiplicatieve functie is, volgt redelijk eenvoudig dat dit inderdaad een multiplicatief karakter vormt. We kunnen verder inzien dat ieder niet-triviaal multiplicatief karakter van orde twee het Legendresymbool is. Stel $\chi$ is een karakter van orde twee. Laat $a \in \mathbb{F}_p^*$ een kwadraatrest zijn, dan geldt uiteraard $\chi(a) = 1$. Laat $b \in \mathbb{F}_p^*$. Stel dat $a$ geen kwadraatrest is, dan volgt dat elke niet-kwadraatrest van de vorm $ab$ is waar $b$ een kwadraatrest is. Echter, dan volgt $\chi(ab) = 1$, dus $\chi$ is triviaal. Derhalve moet gelden $\chi(a) = -1$. We zullen later de Gauss-sommen bekijken met dit karakter, deze sommen worden de kwadratische Gauss-sommen genoemd.

## 2.2 Gauss-sommen op $\mathbb{F}_p$

Met de definities van karakters zijn we nu in staat om Gauss-sommen te definiëren. Eerst worden Gauss-sommen op het eindige lichaam $\mathbb{F}_p$ gedefinieerd, met $p$ een priemgetal.

**Definitie 2.2.1.** Laat $\chi$ een multiplicatief karakter en $\psi$ een additief karakter zijn. Dan is de som $\sum_{a\in\mathbb{F}_p^*}\chi(a)\psi(a)$ de Gauss-som op $\mathbb{F}_p$.

Om de Gauss-sommen op dit lichaam te kunnen bekijken, ligt het voor de hand om een expliciete uitdrukking te geven aan het additieve karakter op dit lichaam. Dit doen we door gebruik te maken van het volgende elementaire lemma.

**Lemma 2.2.1.** *Ieder additief karakter $\psi$ op $\mathbb{F}_p$ is van de vorm $\psi_a(t) = exp(\frac{2\pi iat}{p})$.*

*Bewijs.* Laat $\psi$ een additief karakter zijn. Uit de additiviteit van $\psi$ volgt dat $\psi(t) = \psi(1)^t$. Omdat $\psi(1)^p = \psi(0) = 1$, volgt nu dat $\psi(1) = exp(\frac{2\pi ia}{p})$ voor een $a \in \mathbb{F}_p$. Het gevraagde volgt nu. □

We gebruiken de notatie $\tau(\chi, \psi_a)$ voor de Gauss-som met multiplicatief karakter $\chi$ en additief karakter $\psi_a$.

We werken nu toe naar het enigszins verrassende resultaat dat de modulus van de Gauss-som op $\mathbb{F}_p$ gelijk is aan $\sqrt{p}$. We hebben hiertoe wat lemma's nodig. Ten eerste kunnen we met behulp van het volgende lemma ons beperken tot de Gauss-sommen $\tau(\chi, \psi_1)$ die we $\tau(\chi)$ zullen noemen.

**Lemma 2.2.2.** *Laat $a \in \mathbb{F}_p^*$, dan volgt: $\tau(\chi, \psi_a) = \overline{\chi(a)}\tau(\chi)$.*

*Bewijs.* Stel $y = at$. We vinden nu: $\tau(\chi, \psi_a) = \sum_{t=1}^{p-1}\chi(t)\psi_a(t) = \sum_{y=1}^{p-1}\chi(ya^{-1})\psi_1(y) = \chi(a^{-1})\sum_{y=1}^{p-1}\chi(y)\psi_1(y) = \overline{\chi(a)}\tau(\chi)$. □

**Stelling 2.2.3.** *Laat $\chi$ een niet-triviaal karakter op $\mathbb{F}_p$ zijn, dan geldt $|\tau(\chi)| = \sqrt{p}$.*

*Bewijs.* We bekijken eerst $\overline{\tau(\chi)} = \sum_{t=1}^{p-1}\overline{\chi(t)\psi_1(t)} = \sum_{t=1}^{p-1}\overline{\chi(t)}\psi_1(-t)$. Vermenigvuldiging van zowel het linker- als rechterlid met $\tau(\chi)$ en toepassing van het vorige lemma levert: $|\tau(\chi)|^2 = \sum_{t=1}^{p-1}\tau(\chi, \psi_t)\psi_1(-t) = \sum_{t=1}^{p-1}\sum_{x=1}^{p-1}\chi(x)\psi_1(tx)\psi_1(-t) = \sum_{x=1}^{p-1}\chi(x)\sum_{t=1}^{p-1}\psi_1(t(x-1))$. Omdat voor $x \neq 1$ het karakter $t \to \psi_1(t(x-1))$ niet-triviaal is, volgt uit propositie 2.1.2 dat $\sum_{t=0}^{p-1}\psi_1(t(x-1)) = 0$. Er volgt nu dat $\sum_{t=1}^{p-1}\psi_1(t(x-1)) = -\psi_1(0) = -1$ als $x \neq 1$ en deze som is gelijk aan $p-1$ als $x = 1$. We vinden nu dat $|\tau(\chi)|^2 = \sum_{x=2}^{p-1} -\chi(x) + \chi(1)(p-1)$, wederom uit propositie 2.1.2 volgt dat $|\tau(\chi)|^2 = p$. Het gevraagde volgt nu. □

**Gevolg 2.2.4.** *Laat $a \in \mathbb{F}_p^*$, dan volgt $|\tau(\chi, \psi_a)| = \sqrt{p}$*

*Bewijs.* Dit volgt uit lemma 2.2.2 en stelling 2.2.3, immers $|\tau(\chi, \psi_a)| = |\overline{\chi(a)}||\tau(\chi)| = |\tau(\chi)| = \sqrt{p}$. □

Om stelling 2.2.3 te bewijzen is het noodzakelijk dat zowel het additieve en multiplicatieve karakter niet-triviaal is. Dit wordt samengevat in het onderstaande lemma.

**Lemma 2.2.5.** *Als $\psi$ een triviaal additief karakter is en $\chi$ een niet-triviaal multiplicatief karakter, dan volgt $\tau(\chi, \psi) = 0$. Als $\chi$ een triviaal multiplicatief karakter is en $\psi$ een triviaal additief karakter, dan volgt $|\tau(\chi, \psi)| = p - 1$.*

**Lemma 2.2.6.** *Laat $\chi$ en $\psi$ niet-triviale karakters zijn, dan geldt $\tau(\chi^{-1}, \psi)\tau(\chi, \psi) = \chi(-1)\sqrt{p}$.*

*Bewijs.* Dit volgt eenvoudig door gebruik te maken van propositie 2.1.1.

$$\tau(\chi^{-1}, \psi) = \sum_{x=1}^{p-1} \chi(x)\overline{\psi(x)} = \sum_{y=1}^{p-1} \chi(-y)\overline{\psi(y)} = \chi(-1)\tau(\chi, \psi)$$

Vermenigvuldiging van zowel het linker- als rechterlid met $\tau(\chi, \psi)$ geeft met behulp van gevolg 2.2.4 volgt nu het gevraagde resultaat. □

## 2.3 Spoor van een algebra

Om Gauss-sommen op $\mathbb{F}_q$ te definiëren, hebben we een additief karakter nodig op dit lichaam. Dit komt erop neer dat we een $\mathbb{F}_p-$lineaire afbeelding moeten vinden van $\mathbb{F}_q$ naar $\mathbb{F}_p$. Zo'n lineaire afbeelding is het "spoor"van een algebra. We zullen zien dat iedere lineaire afbeelding van deze vorm is. Om dit te kunnen definiëren, bekijken we de onderstaande afbeelding. $L$ is een algebra over een eindig lichaam $K$ met $dim_K(L) < \infty$.

$$m_\alpha \colon L \to L$$
$$m_\alpha(x) = \alpha x$$

Deze afbeelding kan geïnterpreteerd worden als vermenigvuldiging met $\alpha$. We kunnen eenvoudig nagaan dat dit een lineaire transformatie is van de vectorruimte $L$ naar zichzelf.

**Definitie 2.3.1.** Laat $m_\alpha$ de afbeelding zoals boven gedefinieerd is, dan is het spoor van $\alpha$ het spoor van de lineaire afbeelding $m_\alpha$. Notatie: $Tr_{L/K}(\alpha)$.

Allereerst moet opgemerkt worden dat de spoorafbeelding $Tr_{L/K}$ welgedefinieerd is, dat wil in dit geval zeggen dat de waarde van het spoor onafhankelijk is van de keuzes voor de basis van $L$ over $K$. Dit kunnen we als volgt inzien: Laat $m_\alpha^B$ en $m_\alpha^{B'}$ de afbeeldingen zijn zoals boven gedefinieerd ten opzichte van de bases $B$ en $B'$, dan bestaat er een transformatiematrix $T$ zodat $m_\alpha^B = Tm_\alpha^{B'}T^{-1}$. Omdat voor het spoor geldt $Tr(AB) = Tr(BA)$ voor matrices $A$ en $B$, geldt nu $Tr(m_\alpha^B) = Tr(Tm_\alpha^{B'}T^{-1}) = Tr(TT^{-1}m_\alpha^{B'}) = Tr(m_\alpha^{B'})$.
Hieronder zien we enkele algemene eigenschappen van het spoor:

**Propositie 2.3.1.** *Laat $\alpha$, $\beta \in L$ en $\lambda \in K$, dan volgt:*

*(i)* $Tr_{L/K}(\alpha) \in K$.

*(ii)* $Tr_{L/K}(\alpha + \beta) = Tr_{L/K}(\alpha) + Tr_{L/K}(\beta)$

*(iii)* $Tr_{L/K}(\lambda\alpha) = \lambda Tr_{L/K}(\alpha)$

*(iv)* $Tr_{L/K}(\lambda) = [L : K]\lambda$

*Bewijs.* $(i)$ volgt uit het feit dat $m_\alpha$ een $K$-lineaire afbeelding is. De bijbehorende matrix bij $m_\alpha$ heeft derhalve coëfficiënten in $K$, er volgt dat $Tr_{L/K}(\alpha) \in K$. De punten $(ii)$ en $(iii)$ volgen, met de lineariteit van $m_\alpha$, uit de algemene eigenschappen van het spoor uit de lineaire algebra. Om $(iv)$ te bewijzen merken we op dat we $m_\lambda$ kunnen interpreteren als de matrix $\lambda I_L$, welke als spoor $\lambda$ heeft. □

**Voorbeeld.** Beschouw het lichaam $K = \mathbb{Q}$ en een eindige uitbreiding van graad twee $L = \mathbb{Q}(\sqrt{d})$, waarbij $d$ geen kwadraat is. Ieder element $\alpha \in L$ kunnen we schrijven als $a_0 + a_1\sqrt{d}$, waar $a_0$,$a_1 \in K$. Om $m_\alpha$ te bekijken is het, vanwege de lineariteit, voldoende om ons te beperken tot vermenigvuldiging met 1 en $\sqrt{d}$ (de basis van $L$). Dit geeft:

$$(a_0 + a_1\sqrt{d})1 = a_0 + a_1\sqrt{d}$$
$$(a_0 + a_1\sqrt{d})\sqrt{d} = a_1 d + a_0\sqrt{d}$$

$m_\alpha$ kan nu dus geschreven worden als de matrix:

$$\begin{pmatrix} a_0 & da_1 \\ a_1 & a_0 \end{pmatrix}$$

Deze matrix heeft spoor $2a_0$, dus $Tr_{L/K}(\alpha) = 2a_0$.

We beperken ons nu tot eindige lichaamsuitbreidingen. Er blijkt een verband te bestaan tussen het minimaal polynoom van $\alpha$ en de karakteristieke vergelijking van $m_\alpha$. We gebruiken de volgende lemma's:

**Lemma 2.3.2.** *Laat $L/K$ een eindige lichaamsuitbreiding zijn, $\alpha \in L$, en $E$ een deellichaam van $L$ dat $K$ bevat en $\alpha \in E$. Laat $P_\alpha$ het karakteristieke polynoom van $m_\alpha$ zijn ($P_\alpha(x)$ is dus gelijk aan $det(m_\alpha - xI)$). Laat $m'_\alpha$ de restrictie zijn van $m_\alpha$ tot $E$, en $Q_\alpha$ het karakteristieke polynoom van $m'_\alpha$. Dan volgt:*

$$P_\alpha = Q_\alpha^{[L:E]} \tag{2.1}$$

*Bewijs.* Laat $\{v_1, ..., v_m\}$ een basis zijn van $E$ over $K$, en $\{w_1, ..., w_n\}$ een basis van $L$ over $E$. Omdat $\alpha \in E$ kunnen we $\alpha v_i$ schrijven als $\sum_{j=1}^{m} a_{ij} v_j$, voor zekere $a_{ij} \in K$ en $1 \leq i \leq m$. We kunnen nu dus de vermenigvuldiging $\alpha v_i w_j$ schrijven als $\sum_{k=1}^{m} a_{ik} v_k w_j$ voor elke $1 \leq j \leq n$. De verzameling $\{v_i w_j | 1 \leq i \leq m, 1 \leq j \leq n\}$ vormt een basis van L over K. We kunnen nu dus kijken naar de lineaire afbeelding $m_\alpha$ die we kunnen interpreteren als een $mn \times mn$-matrix. Als de basis lexicografisch geordend wordt, dan komen op de diagonaal de $n \times n$-blokken $m'_\alpha$.

$$\begin{pmatrix} m'_\alpha & 0 & \dots & 0 \\ 0 & m'_\alpha & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & m'_\alpha \end{pmatrix}$$

Met behulp van de eigenschappen van de determinant is eenvoudig na te gaan dat $P_\alpha(x) = det(m_\alpha - xI_{mn}) = det(m'_\alpha - xI_n)^m = Q_\alpha^{[L:E]}(x)$. Hiermee is het gevraagde aangetoond. □

In het volgende lemma beschrijven we een verband tussen het minimale polynoom van $\alpha$ en de karakteristieke vergelijking van $m_\alpha$.

**Lemma 2.3.3.** *Laat $K(\alpha)$ een lichaamsuitbreiding van $K$. Laat $P_\alpha$ het karakteristieke polynoom van $m_\alpha$ zijn en $f_\alpha$ het minimale polynoom van $\alpha$. Dan geldt:*

$$P_\alpha = f_\alpha \tag{2.2}$$

*Bewijs.* Met behulp van de stelling van Cayley-Hamilton (iedere matrix voldoet aan zijn eigen eigenwaardevergelijking) vinden we dat $P_\alpha(m_\alpha) = 0$, dit betekent ook $P_\alpha(\alpha) = 0$. Hieruit volgt dat $f_\alpha$ een deler is van $P_\alpha$. Omdat zowel $f_\alpha$ als $P_\alpha$ monische irreducibele polynomen zijn van dezelfde graad concluderen we het gevraagde. □

**Gevolg 2.3.4.** *Laat $L/K$ een eindige lichaamsuitbreiding zijn, $\alpha \in L$, $P_\alpha$ een karakteristiek polynoom en $f_\alpha$ het minimaalpolynoom van $\alpha$, dan: volgt:*

$$P_\alpha = f_\alpha^{[L:K(\alpha)]} \tag{2.3}$$

*Bewijs.* Dit is een direct gevolg uit de vorige lemma's. Pas lemma 2.3.2 toe op $E = K(\alpha)$ en het gewenste resultaat volgt. □

**Lemma 2.3.5.** *Laat $L/K$ een eindige Galois-uitbreiding zijn, en $m = [L : K]$. Laat $P_\alpha$ het karakteristieke polynoom van $m_\alpha$ zijn dan is $P_\alpha$ te schrijven als:*

$$P_\alpha(x) = \prod_{i=1}^{m}(x - \sigma_i(\alpha)) \tag{2.4}$$

*Waar de $\sigma_i$ de verschillende K-automorfismen zijn op L.*

*Bewijs.* Uit de separabiliteit van $L/K$ volgt dat er onder de geconjungeerden $\sigma_1(\alpha), ..., \sigma_n(\alpha)$ precies $[K(\alpha) : K]$ verschillende automorfismen zijn en elk van deze geconjungeerden is precies $[L : K(\alpha)]$ keer herhaald. De gelijkheid volgt nu met behulp van het vorige lemma.

□

Nu koppelen we het spoor van $\alpha$ aan de automorfismen van $L$.

**Lemma 2.3.6.** *Laat $L, K$ en $\alpha$ als boven, dan geldt:*

$$Tr_{L/K}(\alpha) = \sum_{i=1}^{m} \sigma_i(\alpha)$$

*Bewijs.* Om dit te kunnen bewijzen, werken we eerst het linkerlid uit. Omdat $P_\alpha(x)$ het karakteristieke polynoom van $m_\alpha$ is, is het spoor van deze matrix precies de coëfficiënt van de term $x^{m-1}$. Het uitwerken van het rechterlid levert als coëfficiënt van de term $x^{m-1}$ van $P_a(x)$ gelijk aan $\sum_{i=0}^{m} \sigma_i(\alpha)$. Met behulp van lemma 2.3.5 concluderen we nu het gevraagde. □

Met behulp van de vorige gelijkheid kunnen we laten zien dat het spoor van een eindige lichaamsuitbreiding nooit de nulfunctie kan zijn. Hiervoor hebben we de stelling van Dedekind nodig.

**Lemma 2.3.7** (Dedekind)**.** *Laat $L$ een lichaam zijn en $\sigma_1, ..., \sigma_r$ verschillende automorfismen van $L$. Stel dat er $a_1, ..., a_r \in L$ zijn zodat Voor alle $x \in L$:*

$$\sum_{i=1}^{r} a_i\sigma_i(x) = 0$$

*dan moet volgen $a_1 = a_2 = ... = a_r = 0$.*

*Bewijs.* We volgen het bewijs van [2]. Dit lemma kan bewezen worden met inductie naar $r$. Voor $r = 1$ is de stelling waar. Immers, als we $x = 1$ invullen, dan vinden we dat $a_1\sigma_1(1) = a_1$. Dus $a_1 = 0$. Laat $r > 1$ en neem aan dat de stelling waar is voor elk $(r - 1)$-tupel automorfismen. Kies nu een automorfisme $\sigma_i$ waar $i < r$, dan bestaat er, omdat $\sigma_i$ en $\sigma_r$ verschillend zijn, een $\beta \in L$ zodat $\sigma_i(\beta) \neq \sigma_r(\beta)$.

Omdat voor alle $x \in L$ volgt dat $a_1\sigma_1(x) + a_2\sigma_2(x) + ... + a_r\sigma_r(x)$, volgt zeker ook dat $a_1\sigma_1(\beta x) + a_2\sigma_2(\beta x) + ... + a_r\sigma_r(\beta x)$ voor alle $x \in L$. Als we nu van deze uitdrukking $\sigma_r(\beta)$ maal de eerste uitdrukking afhalen, dan krijgen we de vergelijking

$$a_1(\sigma_1(\beta) - \sigma_r(\beta)) + a_2(\sigma_2(\beta) - \sigma_r(\beta)) + ... + a_{r-1}(\sigma_{r-1}(\beta) - \sigma_r(\beta)) = 0$$

voor alle $x \in L$. Volgens de inductiehypothese concluderen we nu dat alle coëffciënten van deze vergelijking nul moeten zijn, dus in het bijzonder $a_i(\sigma_i(\beta) - \sigma_r(\beta)) = 0$. Omdat $\beta$ gekozen is zodanig dat $\sigma_i(\beta) - \sigma_r(\beta) \neq 0$ moet volgen dat $a_i = 0$. Omdat $i$ willekeurig gekozen is volgt nu automatisch $a_i = 0$ voor alle $i < r$. Er volgt nu $a_r\sigma_r(x) = 0$ voor alle $x \in L$, het invullen van $x = 1$ in de laatste vergelijking levert $a_r = 0$. □

**Gevolg 2.3.8.** *Laat $L/K$ een eindige Galois-uitbreiding zijn. Dan bestaat er een $b \in L$ zodat $Tr_{L/K}(b) \neq 0$.*

*Bewijs.* Stel dat voor alle $b \in L$ geldt dat $Tr_{L/K}(b) = 0$, dan is dit in tegenspraak met het vorige lemma als we $a_1 = ... = a_n = 1$ kiezen. □

Deze eigenschappen van het spoor kunnen ook toegepast worden op het lichaam $K = \mathbb{F}_p$ en de eindige uitbreiding $L = \mathbb{F}_q$. De groep van lichaamsautomorfismen op $L$ is cyclisch en gegenereerd door het Frobenius-automorfisme $\sigma_p \colon x \to x^p$.

**Gevolg 2.3.9.** *Laat $L = \mathbb{F}_{p^n}$ en $K = \mathbb{F}_p$, dan volgt dat*

$$Tr_{\mathbb{F}_q/\mathbb{F}_p}(x) = \sum_{i=0}^{n-1} x^{p^i}$$

**Lemma 2.3.10.** *Laat $K$ een lichaam zijn, en $A$ en $B$ algebra's over het lichaam $K$. Dan volgt $Tr_{(A\times B)/K} = Tr_{A/K} + Tr_{B/K}$.*

*Bewijs.* Dit kan worden ingezien door op te merken dat we $m_{A\times B}$ kunnen schrijven als $\begin{pmatrix} m_A & 0 \\ 0 & m_B \end{pmatrix}$. Het spoor van deze matrix is dus $Tr_{A/K} + Tr_{B/K}$. □

## 2.4 Gauss-sommen op $\mathbb{F}_q$

We kunnen de definitie van Gauss-sommen op $\mathbb{F}_p$ ook uitbreiden tot $\mathbb{F}_q$, waar $q = p^n$.

**Definitie 2.4.1.** Laat $L = \mathbb{F}_q$. Laat $\psi$ een additief karakter en $\chi$ een multiplicatief karakter op $L$ zijn. Dan is

$$\tau(\chi, \psi) = \sum_{a \in L^*} \chi(a)\psi(a)$$

de Gauss-som op het lichaam $L$.

Net als bij additieve karakters van het lichaam $\mathbb{F}_p$, kan bij het lichaam $\mathbb{F}_q$ een vaste uitdrukking gevonden worden. Hiervoor moeten eerst enkele lemma's bewezen worden.

**Lemma 2.4.1.** *Laat $L = \mathbb{F}_q$, $K = \mathbb{F}_p$ en $b \in \mathbb{F}_q$. Dan is de afbeelding*

$$\psi_b \colon a \to exp\left(\frac{2\pi i Tr_{L/K}(ab)}{p}\right)$$

*een additief karakter op $L$.*

*Bewijs.* Dit volgt eenvoudig uit de lineariteit van $Tr_{L/K}$. □

**Lemma 2.4.2.** *Laat $L = \mathbb{F}_q$, $K = \mathbb{F}_p$ en $b \in \mathbb{F}_q$. Dan volgt dat de afbeelding*

$$\begin{aligned} \theta \colon L &\to \widehat{L} \\ b &\to \psi_b \end{aligned}$$

*bijectief is.*

*Bewijs.* Met behulp van propositie 2.1.4 is het voldoende te bewijzen dat $\theta$ injectief is. Omdat $\theta$ een groepshomomorfisme is, is het voldoende te laten zien dat $Ker(\theta) = \{\psi_0\}$. Merk op dat $b \in Ker(\theta)$ precies als voor alle $a \in L$ geldt $Tr_{L/K}(ab) = 0$. Echter, uit gevolg 2.3.8 volgt dat er een $c \in L$ bestaat zodat $Tr_{L/K}(c) \neq 0$. Er moet nu geconcludeerd worden dat $b = 0$, dus $Ker(\theta) = \{\psi_0\}$. □

De eigenschappen van Gauss-sommen op $\mathbb{F}_p$ zijn vergelijkbaar met de eigenschappen van Gauss-sommen op $\mathbb{F}_q$. De bewijzen zijn voor beide lichamen volledig analoog. We zullen dus kort de eigenschappen van Gauss-sommen op $\mathbb{F}_q$ benoemen zonder bewijs.

**Stelling 2.4.3.** *Laat $\psi$ een niet-triviaal additief karakter zijn en $\chi$ een niet- triviaal multiplicatief karakter, dan $|\tau(\chi, \psi)| = \sqrt{q}$.*

**Lemma 2.4.4.** *Als $\psi$ een triviaal additief karakter is en $\chi$ een niet-triviaal multiplicatief karakter, dan volgt $\tau(\chi, \psi) = 0$. Als $\chi$ een triviaal multiplicatief karakter is en $\psi$ een niet-triviaal additief karakter dan $|\tau(\chi, \psi)| = p - 1$.*

**Lemma 2.4.5.** *Laat $\psi$ een additief karakter zijn en $\chi$ een multiplicatief karakter, dan geldt:*

$$\tau(\chi^{-1}, \psi)\tau(\chi, \psi) = \chi(-1)\sqrt{q}.$$

# Hoofdstuk 3

# Gauss-sommen op $\mathbb{F}_q[X]/(f(X))$

## 3.1 Algemene Gauss-sommen

In deze paragraaf laten we zien hoe we de berekening van Gauss-sommen op $\mathbb{F}_q[X]/(f(X))$, waar $f(X) \in \mathbb{F}_q[X]$, kunnen beperken tot Gauss-sommen van de vorm $\mathbb{F}_q[X]/(g(X)^m)$ waar $g$ een irreducibel polynoom is.

**Stelling 3.1.1** (Chinese reststelling)**.** *Laat $R$ een commutatieve ring zijn met eenheidselement, laat $I_1, I_2, ..., I_n$ idealen die paarsgewijs priem zijn(d.w.z. $I_i + I_j = R$ voor alle $i \neq j$) en $I = I_1 \cdot I_2 \cdot ... \cdot I_n$. Dan geldt het volgende isomorfisme:*

$$R/I \simeq R/I_1 \times R/I_2 \times ... \times R/I_n \tag{3.1}$$

*Bewijs.* Zie [2]. □

Beschouw nu de ring $R = \mathbb{F}_q[X]$ en $f(X) \in R$, dan kunnen we $f$ ontbinden in irreducibele factoren, $f[X] = f_1(X)^{e_1}...f_n(X)^{e_n}$. Nu vormen de idealen $(f_i(X)^{e_i})$ paarsgewijze priemidealen, en kunnen we de Chinese reststelling hierop toepassen.

**Gevolg 3.1.2.** *Laat $f_i$ voor $0 \leq i \leq n$ de irreducibele factoren van $f$ zijn dan geldt het volgende isomorfisme:*

$$\mathbb{F}_q[X]/(f(X)) \simeq \mathbb{F}_q[X]/(f_1(X)^{e_1}) \times \mathbb{F}_q[X]/(f_2(X)^{e_2}) \times ... \times \mathbb{F}_q[X]/(f_n(X)^{e_n}) \tag{3.2}$$

Om Gauss-sommen op deze algebra te bekijken, bepalen we eerst de karakters. Uit de Chinese reststelling blijkt het volgende:

**Lemma 3.1.3.** *Laat $\chi$ een multiplicatief karakter op $\mathbb{F}_q[X]/(f(X))$ zijn en $a \in \mathbb{F}_q[X]/(f(X))$. Schrijf $a$, met behulp van het vorige gevolg, als $(a_1, a_2, ..., a_n)$ waar $a_i \in \mathbb{F}_q[X]/(f_i(X)^{e_i})$. Dan geldt*

$$\chi(a) = \chi_1(a_1)\chi_2(a_2)...\chi_n(a_n) \tag{3.3}$$

*waar $\chi_i$ de afbeelding $a_i \mapsto \chi(1_1, ..., 1_{i-1}, a_i, 1_{i+1}, .., 1_n)$ is.*

*Bewijs.* Met behulp van het isomorfisme uit gevolg 3.1.2 en de multiplicatieviteit van $\chi$ vinden we dat $\chi(a) = \chi((a_1, a_2, ..., a_n)) = \prod_{i=1}^{n} \chi((1_1, 1_2, ..., a_i 1_i, ..., 1_n))$ waar $1_i$ de identiteit is van de ring $\mathbb{F}_q[X]/(f_i(X)^{e_i})$. Merk nu op dat de afbeelding $a_i \to \chi((1_1, 1_2, ..., a_i 1_i, ..., 1_n))$ een multiplicatief karakter induceert op $\mathbb{F}_q[X]/(f_i(X)^{e_i})$. □

Een analoog resultaat vinden we ook voor additieve karakters.

**Lemma 3.1.4.** *Laat $\psi$ een additieve karakter op $\mathbb{F}_q[X]/(f(X))$ zijn en $a \in \mathbb{F}_q[X]/(f(X))$, schrijf $a$ als $(a_1, a_2, ..., a_n)$ waar $a_i \in \mathbb{F}_q[X]/(f_i(X)^{e_i})$. Dan geldt*

$$\psi(a) = \psi_1(a_1)\psi_2(a_2)...\psi_n(a_n) \tag{3.4}$$

**Gevolg 3.1.5.** *Met dezelfde notatie als boven, laat $\tau(\chi, \psi)$ de Gauss-som zijn op $\mathbb{F}_q[X]/(f(X))$ en $\tau(\chi_i, \psi_i)$ de Gauss-sommen op $\mathbb{F}_q[X]/(f_i(X)^{e_i})$. Dan geldt*

$$\tau(\chi, \psi) = \prod_{i=1}^{n} \tau(\chi_i, \psi_i) \tag{3.5}$$

Om de formuleringen van stellingen over Gauss-sommen te vereenvoudigen is de volgende definitie van belang:

**Definitie 3.1.1.** Laat A en B algebra's zijn en $\phi\colon A \to B$ niet injectief. Laat $\phi^*\chi\colon A^* \to \mathbb{C}^*$ de afbeelding zijn, gegeven door $a \to \chi_B(\phi(a))$, waar $\chi_B$ een multiplicatief karakter is op $B^*$. Een multiplicatief karakter $\chi$ heet *primitief* als $\chi$ niet van de vorm $\phi^*\chi_B$ is.

Hieronder volgt een voorbeeld van een niet-primitief karakter:

**Voorbeeld** Laat A $= \mathbb{Z}/20\mathbb{Z}$. Laat $\chi$ een multiplicatief karakter zijn op $A$, triviaal op de algebra $\mathbb{Z}/5\mathbb{Z}$. Met de Chinese reststelling schrijven we $a \in A^*$ als $(a_1, a_2)$, waarin $a_1 \in \mathbb{Z}/5\mathbb{Z}$ en $a_2 \in \mathbb{Z}/4\mathbb{Z}$. Omdat geldt dat $\chi(a) = \chi_1(a_1)\chi_2(a_2) = \chi_2(a_2)$ voor karakters $\chi_1$ en $\chi_2$, bestaat er nu een surjectieve functie $\phi$ zodat $\chi = \phi^*\chi_2$. Namelijk $\phi\colon a \to a \bmod 4$. Er volgt dat $\chi$ niet-primitief is.

**Lemma 3.1.6.** *Als $\chi$ een primitief karakter is, dan volgt (met notatie als boven) dat elke $\chi_i$ niet-triviaal is.*

*Bewijs.* Stel dat $\chi_i$ een triviaal karakter is. Met de Chinese reststelling volgt dat $\mathbb{F}_q[X]/(f(X)) \simeq \mathbb{F}_q[X]/(f_i(X)^{e_i}) \times \mathbb{F}_q[X]/(f_1(X)^{e_1}...f_{i-1}(X)^{e_{i-1}} f_{i+1}(X)^{e_{i-1}}...f_n(X)^{e_n})$. Laat $\phi$ nu de afbeelding

$$a \to a \bmod (f_i^{e_i})$$

zijn met $a \in \mathbb{F}_q[X]/(f(X))$. Dan volgt dat $\chi(a) = \chi'(\phi(a))$, waar $\chi'$ een multiplicatief karakter is op $\mathbb{F}_q[X]/(f_1(X)^{e_1}...f_{i-1}(X)^{e_{i-1}} f_{i+1}(X)^{e_{i-1}}...f_n(X)^{e_n})$. □

**Lemma 3.1.7.** *Laat $A = \mathbb{F}_q[X]/(f(X)^n)$. Als $\chi$ een primitief karakter is, dan volgt dat $\chi$ niet-triviaal is op $1 + (f(X))^{n-1}$.*

*Bewijs.* Stel dat $\chi$ triviaal is op $1 + (f(X)^{n-1})$. Laat $a \in A^*$, dan bestaan er een $b \in \mathbb{F}_q[X]/(f(X)^{n-1})$ en $c \in (\mathbb{F}_q[X]/(f(X)))^*$, zodat $\chi(a) = \chi(b)\chi(1 + cf(X)) = \chi(b)$. Dit geeft dus een niet-injectieve afbeelding naar de algebra $\mathbb{F}_q[X]/(f(X)^{n-1})$. Er volgt dat $\chi$ geen primitief karakter is. Het lemma is hiermee bewezen. □

## 3.2 Gauss-sommen op $\mathbb{F}_q[X]/(f_1(X) \cdot ... \cdot f_n(X))$

Met behulp van de vorige paragraaf kunnen we nu onderzoeken hoe Gauss-sommen er uit zien op algebra's $\mathbb{F}_q[X]/(f_1(X) \cdot ... \cdot f_n(X))$, waar iedere $f_i(X)$ irreducibel is. Met gevolg 3.1.5 vinden we nu dat $\tau(\chi, \psi) = \prod_{i=1}^n \tau(\chi_i, \psi_i)$, waar $\tau(\chi_i, \psi_i)$ een Gauss-som is op $\mathbb{F}_q[X]/(f_i(X))$. Omdat $f_i(X)$ irreducibel is, volgt dat deze ring weer een eindig lichaam is en hierop zijn Gauss-sommen al uitgebreid onderzocht. We kunnen nu dus eenvoudig resultaten afleiden.

**Lemma 3.2.1.** *Er geldt $\tau(\varepsilon, \psi) = (-1)^n$.*

*Bewijs.* We gebruiken gevolg 3.1.5 en we zien dat $\tau(\varepsilon, \psi) = \prod_{i=1}^n \tau(\varepsilon_i, \psi_i) = \prod_{i=1}^n (-1) = (-1)^n$. □

**Lemma 3.2.2.** *Er geldt $\tau(\chi^{-1}, \psi) = \chi(-1)\overline{\tau(\chi, \psi)}$.*

*Bewijs.* We gebruiken gevolg 3.1.5.
$\tau(\chi^{-1}, \psi) = \prod_{i=1}^n \tau(\chi_i^{-1}, \psi_i) = \prod_{i=1}^n \chi_i(-1)\overline{\tau(\chi_i, \psi_i)} = \prod_{i=1}^n \chi_i(-1)\overline{\prod_{i=1}^n \tau(\chi_i, \psi)} = \chi(-1)\overline{\tau(\chi, \psi)}$. □

Net als op eindige lichamen, kunnen we de additieve karakters van deze algebra uitdrukken met behulp van het spoor. Om dit te laten zien moet aangetoond worden dat het spoor op deze algebra niet-triviaal kan zijn.

**Lemma 3.2.3.** *Laat $L = \mathbb{F}_q[X]/(f(X))$, met $q = p^m$, $f$ een separabel polynoom in $\mathbb{F}_q[X]$ en $b \in L$. Als de afbeelding*

$$\phi_b \colon a \to Tr_{L/\mathbb{F}_p}(ab)$$

*de nulafbeelding is, dan moet gelden dat $b = 0$.*

*Bewijs.* Stel dat er een $b \in L$ bestaat ongelijk aan 0, zodat $\phi_b$ de nulafbeelding is. Met behulp van de Chinese reststelling is $L$ isomorf met $\mathbb{F}_q[X]/(f_1(X)) \times ... \times \mathbb{F}_q[X]/(f_n(X))$ waarin elke $f_i$ een irreducibele factor van $f$ is. Onder dit isomorfisme is $b$ te schrijven als $(b_1, ..., b_n)$. Omdat $b \neq 0$, bestaat er een $j$ zodanig dat $b_j \neq 0$. De afbeelding $m_\alpha$ is

onder dit isomorfisme te schrijven als $m_{\alpha_1} \times ... \times m_{\alpha_n}$, met $\alpha_i \in \mathbb{F}_q[X]/(f_i(X))$. Het volgt nu dat voor elke $a \in L$

$$Tr_{L/\mathbb{F}_p}(ab_j) = Tr_{L_j/\mathbb{F}_p}(a_j b_j)$$

waar $L_j = \mathbb{F}_q[X]/(f_j(X))$ en $a_j$ het $j$-e component van $a$ onder het isomorfisme. Er geldt dat $L_j$ een eindige lichaamsuitbreiding is, dus met behulp van gevolg 2.3.8 concluderen we dat, als voor elke $a_j \in L_j$ volgt dat $Tr_{L_j/\mathbb{F}_p}(a_j b_j) = 0$, dan moet volgen dat $b_j = 0$. Dit is in tegenspraak met de vooronderstelling dat $b_j = 0$, dus als $\phi_b$ de nulafbeelding is, concluderen we $b = 0$. □

**Gevolg 3.2.4.** *Laat $\psi_b$ de afbeelding*

$$a \to exp\left(\frac{2\pi i Tr_{\mathbb{F}_q/\mathbb{F}_p}(ab)}{p}\right)$$

*zijn, dan volgt dat de afbeelding*

$$\begin{aligned} \theta\colon L &\to \widehat{L} \\ b &\to \psi_b \end{aligned}$$

*bijectief is.*

*Bewijs.* Omdat $\theta$ een groepshomomorfisme is, is het voldoende om voor de injectiviteit te laten zien dat $Ker(\theta) = \{0\}$. Omdat $\theta$ de eenheidsafbeelding is, precies als $\phi_b$ de nulafbeelding is, kan met behulp van het vorige lemma geconcludeerd worden dat $b = 0$. De injectiviteit van $\theta$ volgt nu. Uit propositie 2.1.4 volgt dat $|L| = |\hat{L}|$, dus we kunnen concluderen dat $\theta$ surjectief, en dus bijectief is. □

**Stelling 3.2.5.** *Met dezelfde notatie als boven. Laat $\chi$ een primitief multiplicatief karakter zijn en $\psi_b$ een additief karakter, dan volgt*

$$|\tau(\chi, \psi_b)| = \begin{cases} \sqrt{L} & \text{als } b \in L^*. \\ 0 & \text{anders.} \end{cases}$$

*Bewijs.* Stel $b \in L^*$. Met behulp van gevolg 3.1.5 vinden we $|\tau(\chi, \psi)| = \prod_{i=1}^{n} |\tau(\chi_i, \psi_i)|$. Nu is $\tau(\chi_i, \psi_i)$ weer een Gauss-som over een eindig lichaam. Met behulp van lemma 2.3.10 kan worden ingezien dat $\psi_b = \psi_{b_1} \cdot ... \cdot \psi_{b_n}$, waarin $b_i \equiv b \bmod f_i(X)$ en $\psi_{b_i}$ het additieve karakter is op het lichaam $L_i$. Omdat $b \in L^*$, volgt dat iedere $b_i \in L_i^*$. Dit betekent dat voor iedere $i$, $\psi_{b_i}$ niet-triviaal is en dus $|\tau(\chi_i, \psi_{b_i})| = \sqrt{L_j}$. Er volgt nu dus $|\tau(\chi, \psi_b)| = \prod_{i=1}^{n} |\tau(\chi_i, \psi_{b_i})| = \sqrt{L}$.
Stel $b \notin L^*$. Dan volgt dat er een $i$ bestaat zodat $b_i \equiv b \bmod f_i(X)$. Hieruit volgt dat $\tau(\chi, \psi_{b_i}) = 0$, omdat $\chi_{b_i}$ triviaal is en $\chi_i$ niet-triviaal. □

# Hoofdstuk 4

# Gauss-sommen op $\mathbb{F}_q[X]/(f(X)^n)$

In dit hoofdstuk zal gekeken worden naar Gauss-sommen op de ring $\mathbb{F}_q/(f(X)^n)$, $n \geq 1$ waar $f(X)$ een irreducibel polynoom is in $\mathbb{F}_q[X]$ . In dit hoofdstuk zal onder andere een algemene formule worden gegeven voor de modulus van de Gauss-som. We zullen eerst wat algemene stellingen behandelen.

**Lemma 4.0.1.** *Laat $R$ een eindige ring zijn met 1. Dan geldt dat ieder element van $R$ ofwel een nuldeler is, ofwel een inverteerbaar element.*

*Bewijs.* Laat $a \in R$ een niet-inverteerbaar element zijn, dan bestaat er geen $x \in R$ zodat $ax = 1$. De afbeelding $x \to ax$ is dus niet surjectief, en omdat $R$ een eindige ring is, volgt dat deze afbeelding niet injectief is. Er bestaan dus $x, y \in R$ met $x \neq y$, zodanig dat $0 = ax - ay = a(x - y)$. Er volgt nu dat $a$ een nuldeler is. □

**Lemma 4.0.2.** *Laat $L = \mathbb{F}_q[X]/(f(X)^n)$. Dan volgt dat $L^* = L - (f(X))$*

*Bewijs.* Laat $a \notin L^*$, dan volgt uit het vorige lemma dat a een nuldeler is. Dus er bestaat een $b \neq 0$ zodat $ab \equiv 0 \bmod f(X)^n$, dus $ab = p(X)f(X)^n$ voor een zekere $p(X) \in \mathbb{F}_q[X]$. Omdat $b \not\equiv 0 \pmod{f(X)^n}$ moet volgen dat er een $r > 1$ bestaat zodat $a \equiv 0 \pmod{f(X)^r}$. Er volgt nu $a \in (f(X))$. Het is eenvoudig na te gaan dat als $a \in (f)$, dat dan volgt $a \notin L^*$. □

In het bijzonder kunnen we nu opmerken dat de verzameling van niet-inverteerbare elementen een additieve groep is. Deze eigenschap blijkt essentieel te zijn om de absolute waarde van Gauss-sommen te berekenen.

## 4.1 Gauss-sommen zonder gespecificeerd additief karakter

In deze paragraaf zullen eigenschappen van Gauss-sommen bekeken worden zonder dat er een vaste uitdrukking is voor het additieve karakter. De volgende stelling geeft de

belangrijkste eigenschap van de Gauss-som weer. Merk op dat dit resultaat analoog is met het resultaat voor eindige lichamen.

**Stelling 4.1.1.** *Laat $A$ de ring $\mathbb{F}_q[X]/(f(X)^n)$ zijn met $f(X)$ een irreducibel polynoom. Laat $\psi$ een additief karakter zijn en laat $\psi$ niet-triviaal zijn op $(f(X)^{n-1})$. Laat $\chi$ een multiplicatief karakter zijn met de eigenschap dat $\chi$ niet-triviaal is op $1+(f(X)^{n-1})$. Dan volgt $|\tau(\chi,\psi)| = \sqrt{|A|}$.*

*Bewijs.* Om dit te bewijzen bestuderen we, net als bij eindige lichamen, de waarde $\tau(\chi,\psi)\overline{\tau(\chi,\psi)}$. Zet nu $t = ab^{-1}$, dan volgt

$$|\tau(\chi,\psi)|^2 = \tau(\chi,\psi)\overline{\tau(\chi,\psi)} = \sum_{a,b\in A^*} \chi(a)\overline{\chi(b)}\psi(a)\overline{\psi(b)} = \sum_{t\in A^*}\chi(t)\sum_{b\in A^*}\psi(b(t-1)).$$

Om deze som uit te rekenen bepalen we voor gegeven $t \in A^*$ de som $\sum_{b\in A^*}\psi(b(t-1))$. We delen de som op de volgende manier op

$$\begin{aligned}\sum_{t\in A^*}\chi(t)\sum_{b\in A^*}\psi(b(t-1)) = {} & \chi(1)\sum_{b\in A^*}\psi(0) \\ & + \sum_{\substack{t\in 1+(f(X)^{n-1})\\ t\neq 1}}\chi(t)\sum_{b\in A^*}\psi(b(t-1)) \\ & + \sum_{\substack{t\in A^*\\ t\notin 1+(f(X)^{n-1})}}\chi(t)\sum_{b\in A^*}\psi(b(t-1)).\end{aligned}$$

Omdat zowel $A$ als $A - A^*$ additieve groepen vormen, is het eenvoudig om hierop het additieve karakter $\psi$ te bekijken. Om deze reden schrijven we telkens $\sum_{b\in A^*}\psi(b(t-1))$ als $\sum_{b\in A}\psi(b(t-1)) - \sum_{b\in A-A^*}\psi(b(t-1))$. Er volgt nu dus

$$\begin{aligned}|\tau(\chi,\psi)|^2 = {} & |A^*| \\ & + \sum_{\substack{t\in 1+(f(X)^{n-1})\\ t\neq 1}}\chi(t)\left(\sum_{b\in A}\psi(b(t-1)) - \sum_{b\in A-A^*}\psi(b(t-1))\right) \\ & + \sum_{\substack{t\in A^*\\ t\notin 1+(f(X)^{n-1})}}\chi(t)\left(\sum_{b\in A}\psi(b(t-1)) - \sum_{b\in A-A^*}\psi(b(t-1))\right).\end{aligned}$$

Als $t \in 1+(f(X)^{n-1})$ en $t \neq 1$, dan volgt er, uit het feit dat $\psi$ niet-triviaal is op $(f(X)^{n-1})$, dat er een $b \in A$ moet zijn zodat $\psi(b(t-1)) \neq 1$. Er volgt dus dat $b \to \psi(b(t-1))$ een niet-triviaal karakter is op de additieve groep $A$. Er volgt met behulp van propositie 2.1.2 dat voor $t \in 1+(f(X)^{n-1})$ geldt $\sum_{b\in A}\psi(b(t-1)) = 0$. Voor $t \in 1+(f(X)^{n-1})$ en $b \in A-A^*$ volgt dat $b \to \psi(b(t-1))$ een triviaal karakter is omdat

$b \in (f(X))$, dus $\sum_{b \in A-A^*} \psi(b(t-1))) = |A-A^*|$. Met vergelijkbare redeneringen volgt dat er voor inverteerbare $t \notin 1+(f(X)^{n-1})$ een $b \in A-A^*$ bestaat zodat $\psi(b(t-1)) \neq 1$. Deze laatste som is gelijk aan 0 met behulp van propositie 2.1.2. We vinden nu dus

$$\begin{aligned} |\tau(\chi,\psi)|^2 &= |A^*| - |A-A^*| \sum_{\substack{t \in 1+(f(X)^{n-1}) \\ t \neq 1}} \chi(t) \\ &= |A^*| - |A-A^*| \left( \sum_{t \in 1+(f(X)^{n-1})} \chi(t) - 1 \right) \end{aligned} \tag{4.1}$$

Omdat $1 + (f(X)^{n-1})$ een multiplicatieve groep is, en $\chi$ is een niet-triviaal karakter op deze groep, volgt met propositie 2.1.2

$$|\tau(\chi,\psi)| = \sqrt{|A|}.$$

□

**Gevolg 4.1.2.** *Als $\chi$ triviaal is op $1+(f(X)^{n-1})$ en $\psi$ niet-triviaal op $(f(X)^{n-1})$, dan volgt $\tau(\chi,\psi) = 0$.*

*Bewijs.* Dit kan eenvoudig worden nagegaan door op te merken dat $|1+(f(X)^{n-1})| = q^{deg(f(X))}$, dus uit (4.1) volgt nu $|\tau(\chi,\psi)| = \sqrt{|A| - q^{deg(f(X))}|A-A^*|}$. Merk op dat geldt $|A| = q^{deg(f(X))}|A-A^*|$, dus $\tau(\chi,\psi) = 0$. □

Met de vorige stelling is dus een resultaat verkregen dat vergelijkbaar is met resultaten voor eindige lichamen. Het probleem met deze stelling is dat hieruit niet duidelijk blijkt wat er gebeurt als $\psi$ triviaal is op $(f(X)^{n-1})$. Er moet dus gezocht worden naar een concrete uitdrukking voor de additieve karakters. In de volgende paragraaf wordt hiertoe een poging gedaan.

## 4.2 Gauss-sommen met spoorkarakter

Naar analogie van Gauss-sommen over eindige lichamen en algebra's van de vorm $\mathbb{F}_q[X]/(f(X))$ waar $f(X)$ separabel, rijst het vermoeden dat ieder additief karakter op de algebra $A = \mathbb{F}_q[X]/(g(X)^n)$ van de vorm

$$\psi_b \colon a \to exp\left(\frac{2\pi i Tr_{A/\mathbb{F}_p}(ab)}{p}\right)$$

is, met $b \in A$. Met het volgende voorbeeld blijkt dat dit vermoeden onjuist is. Een interessante vraag die dan overblijft is of we een uitspraak kunnen doen over Gauss-sommen met additieve karakters die wél van de spoorvorm zijn.

**Voorbeeld.** Beschouw de ring $R = \mathbb{F}_p[X]/(X^p)$ met $p$ een priemgetal, dan kan gekeken worden naar het spoor $Tr_{R/\mathbb{F}_p}$. Door de lineariteit van het spoor geldt voor elke $a \in R$ (we schrijven $a = a_0 + a_1X + ... + a_{p-1}X^{p-1}$)

$$Tr_{R/\mathbb{F}_p}(a) = a_0Tr_{R/\mathbb{F}_p}(1) + a_1Tr_{R/\mathbb{F}_p}(X) + ... + a_{p-1}Tr_{R/\mathbb{F}_p}(X^{p-1}).$$

Verder kan eenvoudig worden nagegaan dat $Tr_{R/\mathbb{F}_p}(a)(X^i) = 0$ voor ieder $0 \leq i \leq p-1$. Er kan dus geconcludeerd worden dat het enige additieve karakter dat in de spoorvorm geschreven kan worden het triviale karakter is.

**Lemma 4.2.1.** *Laat $a \in A$ een nilpotent element zijn, dan volgt $Tr_{A/\mathbb{F}_p}(a) = 0$.*

*Bewijs.* Omdat $a$ een nilpotent is, bestaat er een $k \geq 1$ zodat $a^k = 0$. Dan volgt dat de afbeelding $m_a$ , zoals gedefinieerd in paragraaf 2.3, de eigenschap heeft $m_a^k = \mathbf{0}$. Er volgt nu dat de eigenwaarden van $m_a^k$ gelijk zijn aan 0, eenvoudig is in te zien dat de eigenwaarden van $m_a$ ook gelijk moeten zijn aan 0. Omdat het spoor van $m_a$ de som van de eigenwaarden is, volgt $Tr_{A/\mathbb{F}_p}(a) = 0$. □

**Lemma 4.2.2.** *Laat $a \in A$ niet-inverteerbaar zijn, dan is $a$ nilpotent.*

*Bewijs.* Dit volgt eenvoudig uit het feit dat $a \in (f(X))$. □

**Stelling 4.2.3.** *Laat $A = \mathbb{F}_q[X]/(f(X)^n)$ met $Tr_{A/\mathbb{F}_q}$ niet de nulafbeelding. Laat $\psi_x \colon a \to exp\left(\frac{2\pi i Tr_{A/\mathbb{F}_p}(ax)}{p}\right)$, $x \in A^*$ een additief karakter zijn en laat $\chi$ niet-triviaal zijn op $1 + (f(X))$, dan volgt $\tau(\chi, \psi) = 0$.*

*Bewijs.* Op vergelijkbare wijze als in paragraaf 4.1 is te vinden

$$\begin{aligned}|\tau(\chi,\psi)|^2 = &\sum_{t\in 1+(f(X))} \chi(t)\left(\sum_{b\in A}\psi(b(t-1)) - \sum_{b\in A-A^*}\psi(b(t-1))\right)\\ &+ \sum_{t\in A^*, t\notin 1+(f(X))} \chi(t)\left(\sum_{b\in A}\psi(b(t-1)) - \sum_{b\in A-A^*}\psi(b(t-1))\right)\end{aligned}$$

Als $t \in 1+(f(X))$ dan is $b(t-1)$ een nilpotent element. We zien dus dat $\psi(b(t-1)) = 1$ voor elke $b \in A$, er geldt dus dat $\sum_{b\in A^*}\psi(b(t-1)) = |A^*|$. Voor $t \in A^*$, $t \notin 1+(f(X))$ bestaat er, omdat het spoor niet de nulafbeelding is, een $b \in A$ zodat $\psi(b(t-1)) \neq 1$. In dit geval geldt dus $\sum_{b\in A}\psi(b(t-1)) = 0$ en $\sum_{b\in A-A^*}\psi(b(t-1)) = |A - A^*|$. We zien nu dus

$$\begin{aligned}|\tau(\chi,\psi)|^2 = &|A^*|\sum_{t\in 1+(f(X))}\chi(t)\\ &- |A-A^*|\left(\sum_{t\in A^*}\chi(t) - \sum_{t\in 1+(f(X))}\chi(t)\right).\end{aligned}$$

Uit het feit dat $\chi(t)$ niet-triviaal is op $1+(f(X))$ concluderen we dat de $\sum_{t\in A^*}\chi(t) = 0$ en $\sum_{t\in 1+(f(X))}\chi(t) = 0$. Er volgt dus $\tau(\chi, \psi) = 0$. □

**Gevolg 4.2.4.** *Als $\chi$ triviaal is op $1+(f(X))$, maar $\chi$ niet-triviaal op $A^*$. Dan volgt* $|\tau(\chi,\psi)| = \sqrt{|A-A^*|\cdot|A|}$.

*Bewijs.* Dit volgt eenvoudig uit het feit dat $\sum_{t\in A^*}\chi(t) = 0$ en $\sum_{t\in 1+(f(X))}\chi(t) = |1+f(X)| = |A-A^*|$. □

Verder is op te merken dat als $Tr_{A/\mathbb{F}_p}$ de nulafbeelding is, dat dan geldt $\tau(\chi,\psi)=0$ als $\chi$ niet-triviaal is. Onder de aanname dat $Tr_{A/\mathbb{F}_p}$ niet de nulafbeelding is en $b\in A^*$ kan samenvattend geconcludeerd worden

$$\tau(\chi,\psi_b) = \begin{cases} 0 & \text{als } \chi \text{ niet-triviaal is op } 1+(f(X)). \\ \sqrt{|A|\cdot|A-A^*|} & \text{als } \chi \text{ niet-triviaal, maar wel triviaal op } 1+(f(X)). \\ |A-A^*| & \text{als } \chi \text{ triviaal is.} \end{cases}$$

Een interessante vraag die nog overblijft is: Voor welke algebra's $A$ geldt dat $Tr_{A/\mathbb{F}_p}$ de nulafbeelding is?

## 4.3 Gauss-sommen met residukarakter

In deze paragraaf wordt additief karakter geïntroduceerd, zoals gedefinieerd door [6]. We zullen laten zien dat alle additieve karakters van deze vorm zijn en dus kunnen we de modulus van de Gauss-sommen uitrekenen voor algemene additieve karakters. Als $A=\mathbb{F}_q[X]/(f(X)^n)$, met $f(X)$ een irreducibel polynoom en $m = n\cdot deg(f(X))$, dan is een element $a\in A$ te schrijven als:

$$a = a_0 + a_1X + ... + a_{m-1}X^{m-1}$$

voor zekere $a_i\in\mathbb{F}_q$. Dan definiëren we het *residu* van $a$ als $res(a)=a_{m-1}$.

**Lemma 4.3.1.** *Laat $b\in A$, dan is*

$$\psi_b\colon a\to exp\left(\frac{2\pi i Tr_{\mathbb{F}_q/\mathbb{F}_p}(res(ab))}{p}\right)$$

*een additief karakter op $A$.*

*Bewijs.* Dit is eenvoudig na te gaan. Er geldt immers dat de afbeeldingen $Tr_{\mathbb{F}_q/\mathbb{F}_p}$ en $res$ lineair zijn. □

**Lemma 4.3.2.** *De afbeelding*

$$\begin{aligned}\theta\colon A &\to \widehat{A} \\ b &\to \psi_b\end{aligned}$$

*is een bijectie.*

*Bewijs.* Voor injectiviteit is het voldoende om te laten zien dat voor $b \neq 0$ een $a \in A$ te vinden is, zodat $Tr_{\mathbb{F}_q/\mathbb{F}_p}(res(ab)) \neq 0$. $b$ kan uitgedrukt worden als $b_0 + b_1 X + ... + b_{m-1}X^{m-1}$ met $b_i \in \mathbb{F}_q$. Kies nu de grootste $j < m$ zodat $b_j \neq 0$, dan volgt dat er een $r \in \mathbb{F}_q$ bestaat, zodat $Tr_{\mathbb{F}_q/\mathbb{F}_p}(rb_j) \neq 0$. De keuze $a = rX^{n-1-j}$ geeft dan $Tr_{\mathbb{F}_q/\mathbb{F}_p}(res(ab)) \neq 0$. De injectiviteit volgt nu. Met propositie 2.1.4 geldt $|A| = |\widehat{A}|$, dus $\theta$ is bijectief. □

We zullen nu de eigenschappen van de Gauss-som laten zien met dit additieve karakter.

**Stelling 4.3.3.** *Laat $A = \mathbb{F}_q[X]/(f(X)^n)$, laat $\psi_v$ ($v \neq 0$) een additief karakter zijn en laat $s \geq 0$ maximaal zijn zodat $v = f(X)^s p(X)$, dan geldt:*

$$|\tau(\chi, \psi_v)| = \begin{cases} \sqrt{|A| \cdot q^{s \cdot deg(f(X))}} & \text{als } \chi \text{ triviaal is op } 1+(f(X)^{n-s}) \text{ en niet-triviaal op} \\ & 1+(f(X)^{n-s-1}) \\ 0 & \text{anders} \end{cases}$$

*Bewijs.* We splitsen de Gauss-som weer op de volgende manier op:

$$\begin{aligned} |\tau(\chi, \psi_v)|^2 = & \sum_{\substack{t \in A^* \\ t \notin 1+(f(X)^{n-s-1})}} \chi(t)\left(\sum_{b \in A} \psi_v(b(t-1)) - \sum_{b \in A - A^*} \psi_v(b(t-1))\right) \\ & + \sum_{\substack{t \in 1+(f(X)^{n-s-1}) \\ t \notin 1+(f(X)^{n-s})}} \chi(t)\left(\sum_{b \in A} \psi_v(b(t-1)) - \sum_{b \in A - A^*} \psi_v(b(t-1))\right) \\ & + \sum_{t \in 1+(f(X)^{n-s})} \chi(t)\left(\sum_{b \in A} \psi_v(b(t-1)) - \sum_{b \in A - A^*} \psi_v(b(t-1))\right) \end{aligned}$$

We onderscheiden nu de verschillende gevallen.

*Stel $\chi$ is niet-triviaal op $1 + (f(X)^{n-s})$.*
Voor $t \in A^*$ en $t \notin 1 + (f(X)^{n-s-1})$ geldt dat er een $b \in A - A^*$ bestaat zodat $\psi_v(b(t-1)) \neq 1$, deze karaktersommen geven dus waarde 0 met propositie 2.1.2 . Voor $t \in 1 + (f(X)^{n-s-1})$ en $t \notin 1 + (f(X)^{n-s})$ geldt dat er een $b \in A^*$ bestaat zodat $\psi_v(b(t-1)) \neq 1$, maar er volgt dat $\psi_v(b(t-1))$ triviaal is voor elke $b \in A - A^*$. Dus er volgt dat voor deze $t$, $\sum_{b \in A} \psi_v(b(t-1)) - \sum_{b \in A - A^*} \psi_v(b(t-1))) = -|A - A^*|$.

Voor $t \in 1 + (f(X)^{n-s})$ volgt op vergelijkbare wijze $\sum_{b\in A} \psi_v(b(t-1)) - \sum_{b\in A-A^*} \psi_v(b(t-1)) = |A^*|$. Er volgt nu dus:

$$\begin{aligned}|\tau(\chi,\psi_v)|^2 =& -|A-A^*|\Big(\sum_{t\in 1+(f(X)^{n-s-1})}\chi(t) - \sum_{t\in 1+(f(X)^{n-s})}\chi(t)\Big)\\ &+|A^*|\sum_{t\in 1+(f(X)^{n-s})}\chi(t).\end{aligned}$$

Aangezien $\chi$ niet-triviaal is op $1+(f(X)^{n-s})$ en dus in het bijzonder niet-triviaal op $1+(f(X)^{n-s-1})$, volgt dat deze karaktersommen gelijk zijn aan 0. We concluderen $\tau(\chi,\psi_b)=0$.

*Stel dat $\chi$ triviaal is op $1+(f(X)^{n-s})$, maar niet-triviaal op $1+(f(X)^{n-s-1})$.*

We kunnen een vergelijkbare redenering houden als bij het geval dat $\chi$ niet-triviaal is op $1+(f(X)^{n-s})$. Omdat $\chi$ triviaal is op $1+(f(X)^{n-s})$ vinden we

$$\sum_{t\in 1+(f(X)^{n-s})}\chi(t) = |1+(f(X)^{n-s})| = q^{s\cdot deg(f(X))}$$

Omdat $\chi$ niet-triviaal is op $1+(f(X)^{n-s-1})$ vinden we nu:

$$\begin{aligned}|\tau(\chi,\psi_v)|^2 =& -|A-A^*|\Big(-q^{s\cdot deg(f(X))}\Big)\\ &+|A^*|\cdot q^{s\cdot deg(f(X))}.\end{aligned}$$

We vinden nu in dit geval het resultaat:

$$|\tau(\chi,\psi_v)| = \sqrt{|A|\cdot q^{s\cdot deg(f(X))}}.$$

*Stel $\chi$ is triviaal op $1+(f(X)^{n-s-1})$*

Als $\chi$ triviaal is op $1+(f(X)^{n-s-1})$, dan geldt:

$$\sum_{t\in 1+(f(X)^{n-s-1})}\chi(t) = |1+(f(X)^{n-s-1})| = q^{(s+1)\cdot(deg(f(X))}.$$

En aangezien $\chi$ uiteraard ook triviaal is op $1+(f(X)^{n-s})$ volgt nu:

$$\begin{aligned}|\tau(\chi,\psi_v)|^2 =& -|A-A^*|\cdot(q^{(s+1)deg(f(X))} - q^{s\cdot deg(f(X))})\\ &+|A^*|\cdot q^{s\cdot deg(f(X))}\\ =&|A|\cdot q^{s\cdot deg(f(X))} - |A-A^*|\cdot q^{(s+1)deg(f(X))}.\end{aligned}$$

Omdat geldt $|A| = q^{deg(f(X))}|A-A^*|$, moet volgen $\tau(\chi,\psi_v)=0$. □

Het volgende resultaat komt wat meer overeen met de resultaten over eindige lichamen en algebra's over separabele polynomen.

**Gevolg 4.3.4.** *Laat $\psi_v$ het additieve karakter zijn op $A$ waarin $v$ relatief priem is met $f(X)$ (dus $v \in A^*$). Als $\chi$ niet-triviaal is op $1+(f(X)^{n-1})$, dan volgt $|\tau(\chi, \psi_v)| = \sqrt{|A|}$.*

*Bewijs.* Dit volgt uit de vorige stelling door $s = 0$ in te vullen. Immers, $\chi$ is uiteraard triviaal op $1 + (f(X)^n)$. □

Uiteindelijk moet ook het geval $v = 0$ onderzocht worden.

**Lemma 4.3.5.** *Indien $\psi_v$ een triviaal additief karakter is ( dus $v \equiv 0$ mod $f(X)^n$), dan volgt $\tau(\chi, \psi_v) = 0$ als $\chi$ triviaal is en $\tau(\chi, \psi_v) = |A^*|$ als $\chi$ niet-triviaal is.*

*Bewijs.* Als $\psi_v$ triviaal is, dan geldt dus

$$\tau(\chi, \psi_v) = \sum_{t \in A^*} \chi(t) \tag{4.2}$$

Als $\chi$ niet-triviaal is, dan is het duidelijk dat deze som de waarde 0 heeft. Als $\chi$ triviaal is, dan is $\sum_{t \in A^*} \chi(t) = |A^*|$. □

## 4.4 Gauss-sommen op $\mathbb{F}_q[X]/(f(X))$

In hoofdstuk 3 hebben we laten zien dat Gauss-sommen op $A = \mathbb{F}_q[X]/(f(X))$ geschreven kunnen worden als het product van Gauss-sommen op $A_i = \mathbb{F}_q[X]/(f_i(X)^{n_i})$ voor zekere irreducibele factoren $f_i(X)$ van $f(X)$. Laat $k$ het aantal irreducibele factoren zijn. De modulus van Gauss-sommen op $A_i$ is in de vorige paragraaf behandeld. Er geldt dus het volgende lemma:

**Lemma 4.4.1.** *Laat $\tau(\chi, \psi)$ de Gauss-som zijn op $A$, dan volgt dat er $b_i \in A_i$ bestaan zodat $|\tau(\chi, \psi)| = \prod_{i=1}^{k} |\tau(\chi_i, \psi_{b_i})|$, waar $\chi$ en $\psi_{b_i}$ karakters zijn op $A_i$.*

Het bestaan van zulke $b_i$ is dus duidelijk. Deze $b_i's$ kunnen ook op de volgende wijze geconstrueerd worden met behulp van de onderstaande lemma's:

**Lemma 4.4.2.** *Laat $f(X), g(X) \in \mathbb{F}_q[X]$, dan bestaan er $s(X), t(X) \in \mathbb{F}_q[X]$ zodat:*

$$s(X)f(X) + t(X)g(X) = ggd(f(X), g(X))$$

Omdat geldt $ggd(f(X), g(X), h(X)) = ggd(f(X), ggd(g(X), h(X)))$ kan inductief het volgende worden afgeleid:

**Gevolg 4.4.3.** *Laat $f_1(X), ..., f_n(X) \in \mathbb{F}_q[X]$, dan bestaan er $s_1(X), ..., s_n(X) \in \mathbb{F}_q[X]$ zodat:*

$$s_1(X)g_1(X) + ... + s_n(X)g_n(X) = ggd(f_1(X), ..., f_n(X))$$

Als dit vorige gevolg toegepast wordt op de polynomen $g_i(X) = \frac{f(X)}{f_i(X)^{e^{n_i}}}$, dan vinden we dat $ggd(g_1(X), ..., g_k(X)) = 1$. In het bijzonder volgt nu dus dat iedere $h(X) \in F_q[X]$ te schrijven is als

$$h(X) = t_1(X)\frac{f(X)}{f_1(X)^{n_i}} + ... + t_k(X)\frac{f(X)}{f_k(X)^{n_k}} \tag{4.3}$$

Voor zekere $t_i(X) \in \mathbb{F}_q[X]$. Tevens kan opgemerkt worden dat $h(X)$ deelbaar is door $f_i(X)$ precies als $t_i(X)$ deelbaar is door $f_i(X)$. Er geldt nu het volgende lemma:

**Lemma 4.4.4.** *Laat $\psi$ een additief karakter zijn op $A$, dan is $\psi$ van de vorm $\psi_v$ voor een zekere $v \in A$. Verder is $\psi_v(a)$ te schrijven als*

$$\psi_v(a) = \psi_{v_1}(a_1) \cdot ... \cdot \psi_{v_k}(a_k) \tag{4.4}$$

*waarin $a_i \equiv a \ mod \ f_i(X)^{n_i}$ en $v_i \in A_i$, zoals geconstrueerd in 4.3.*

*Bewijs.* Door vergelijking (4.3) modulo $f(X)$ te bekijken kunnen we het residu van $av$ op de volgende wijze opschrijven.

$$res_A(av) = res_A\left(av_1\frac{f(X)}{f_1(X)^{n_1}}\right) + ... + res_A\left(av_k\frac{f(X)}{f_k(X)^{n_k}}\right) \tag{4.5}$$

Vervolgens vormt $res_A\big(av_1\frac{f(X)}{f_i(X)^{n_i}}\big)$ weer een residukarakter modulo $f_i(X)^{n_i}$, we schrijven dit als $res_{A_i}$. We vinden nu dus:

$$res_A(av) = res_{A_1}(a_1v_1) + ... + res_{A_k}(a_kv_k) \tag{4.6}$$

Door nu aan beide kanten het spoor en de exponent te nemen vinden we de gevraagde gelijkheid 4.4. □

Met behulp van de resultaten uit het vorige hoofdstuk kunnen we nu de volgende stelling bewijzen:

**Stelling 4.4.5.** *Laat $\chi$ een primitief karakter zijn en $v \in A^*$. Dan volgt $|\tau(\chi, \psi_v)| = \sqrt{|A|}$.*

*Bewijs.* Om deze stelling te bewijzen merken we allereerst op dat $v \in A^*$ impliceert dat $v$ niet deelbaar is door een van de polynomen $f_1(X), ...f_k(X)$. Hieruit volgt weer dat iedere $v_i$ in vergelijking (4.4) niet deelbaar is door $f_i(X)$, dus dit betekent dat $v_i \in A_i^*$. Uit de primitiviteit van $\chi$ volgt dat $\chi$ niet-triviaal is op $A_i$ voor iedere $1 \leq i \leq k$. Eveneens volgt uit de primitiviteit dat $\chi$ niet-triviaal is op $1+(f(X)_i^{n_i-1})$. Met behulp van gevolg 4.3.4 kan nu geconcludeerd worden dat $|\tau(\chi_i, \psi_{v_i})| = \sqrt{|A_i|}$. Verder kan met behulp van gevolg 3.1.5 geconcludeerd worden

$$|\tau(\chi, \psi)| = \sqrt{|A_1|} \cdot \sqrt{|A_2|} \cdot ... \cdot \sqrt{|A_k|} = \sqrt{|A|}.$$

□

**Stelling 4.4.6.** *Laat $\chi$ primitief karakter zijn en stel $v \notin A^*$. Dan volgt $\tau(\chi, \psi_v) = 0$.*

*Bewijs.* Omdat $v \notin A^*$ bestaat er een $i$ zodat $f_i(X)$ een deler is van $v$. Dit betekent met behulp van vergelijking (4.3) dat $v_i$ deelbaar is door $f_i(X)$ en dus $v_i \notin A_i^*$. Wederom kan met stelling 4.3.3 geconcludeerd worden $\tau(\chi_i, \psi_{v_i}) = 0$. Daaruit volgt zeker ook $\tau(\chi, \psi_v) = 0$. □

# Hoofdstuk 5

# Argument van de Gauss-som

In de vorige hoofdstukken is met name gekeken naar de modulus van de Gauss-sommen. In dit hoofdstuk zal het argument van de Gauss-som onderzocht worden. Een analyse naar het argument van dit soort Gauss-sommen werd ook gedaan door [6]. Eerst introduceren we de kwadratische Gauss-sommen, de Gauss-sommen die oorspronkelijk door Gauss onderzocht zijn, deze blijken belangrijk te zijn in de analyse voor het argument van de Gauss-som. Vanwege grote berekeningen gebruiken we vanaf paragraaf 5.1 de notatie $e(x)$ voor $exp\big(\frac{2\pi ix}{p}\big)$.

## 5.1 Kwadratische Gauss-sommen

Kwadratische Gauss-sommen zijn sommen van de onderstaande vorm

$$\tau(a) = \sum_{n=0}^{p-1} exp\left(\frac{2\pi ian^2}{p}\right) \tag{5.1}$$

waar $p$ een priemgetal is. De kwadratische Gauss-sommen kunnen ook algemener gedefinieerd worden als $p$ geen priemgetal is, maar voor onze analyse is dit niet nodig.

**Lemma 5.1.1.** *Laat $(n/p)$ het Legendre-symbool zijn, dan geldt*

$$\tau(a) = \sum_{m=1}^{p-1} \left(\frac{m}{p}\right) exp\left(\frac{2\pi iam}{p}\right) \tag{5.2}$$

*Bewijs.* Het aantal oplossingen van de congruentie

$$n^2 \equiv m \bmod p$$

is gelijk aan $1 + (m/p)$. Er volgt nu dus

$$\tau(a) = \sum_{n=0}^{p-1} exp\left(\frac{2\pi ian^2}{p}\right) = \sum_{m=0}^{p-1} \left(1 + \left(\frac{m}{p}\right) exp\left(\frac{2\pi iam}{p}\right)\right) = \sum_{m=1}^{p-1} \left(\frac{m}{p}\right) exp\left(\frac{2\pi iam}{p}\right) \tag{5.3}$$

□

Met deze vorige gelijkheid kan eenvoudig worden nagegaan dat $\tau(a) = (a/p)\tau(1)$. Het is dus voldoende om $\tau(1)$ te bepalen. De waarde van $\tau(1)$ kan volledig bepaald worden.

**Stelling 5.1.2.** *Laat $p$ een oneven priemgetal zijn, dan volgt*

$$\tau(1) = \begin{cases} \pm\sqrt{p} & \text{als } p \equiv 1 \bmod 4 \\ \pm i\sqrt{p} & \text{als } p \equiv 3 \bmod 4 \end{cases}$$

*Bewijs.* We schrijven eerst $\chi(x) = (x/p)$, dan volgt met lemma 2.2.6

$$\tau(\chi)\tau(\chi^{-1}) = \chi(-1)p. \tag{5.4}$$

Vervolgens volgt dat $\chi^{-1}(a) = (a^{-1}/p) = (a/p) = \chi(a)$. Verder is bekend dat $\chi(-1) = (-1/p) = (-1)^{\frac{p-1}{2}}$. We vinden nu dus

$$\tau(\chi)^2 = (-1)^{\frac{p-1}{2}}\sqrt{p}. \tag{5.5}$$

Hiermee is de stelling bewezen. □

Het blijkt lastiger om het teken van de Gauss-som te bepalen. Daarvoor geldt de volgende stelling:

**Stelling 5.1.3** (Gauss)**.** *Laat $p$ een oneven priemgetal zijn, dan volgt*

$$\tau(1) = \begin{cases} \sqrt{p} & \text{als } p \equiv 1 \bmod 4 \\ i\sqrt{p} & \text{als } p \equiv 3 \bmod 4 \end{cases}$$

*Bewijs.* Zie [5]. □

### 5.1.1 Algemene kwadratische Gauss-sommen

Voor het berekenen van Gauss-sommen hebben we kwadratische Gauss-sommen in een iets algemenere vorm nodig. Namelijk van de vorm:

$$\tau(a,b) = \sum_{n=0}^{p-1} exp\left(\frac{2\pi i(an^2+bn)}{p}\right) \tag{5.6}$$

**Lemma 5.1.4.** *Laat $p$ een oneven priemgetal zijn en $a \not\equiv 0 \bmod p$, dan volgt:*

$$\tau(a,b) = \tau(1) \cdot \left(\frac{a}{p}\right) e(-4^{-1}a^{-1}b^2) \tag{5.7}$$

*Bewijs.* We splitsen eenvoudig het kwadraat af.

$$\begin{aligned}\tau(a,b) =& \sum_{n=0}^{p-1} e(a(n^2 + a^{-1}b)) \\ =& \sum_{n=0}^{p-1} e(a(n + 2^{-1}a^{-1}b)^2)e(-4^{-1}a^{-1}b^2) \\ =& \sum_{m=0}^{p-1} e(am^2)e(-4^{-1}a^{-1}b^2) \\ =& \tau(1) \cdot \left(\frac{a}{p}\right) e(-4^{-1}a^{-1}b^2)\end{aligned}$$

□

## 5.2 Gauss-sommen mod $X^n$

In deze paragraaf zullen we de waarde van de Gauss-som op de algebra $A = \mathbb{F}_p[X]/(X^n)$ berekenen voor een aantal waarden voor $n$, $p \geq n$. We gebruiken hierbij dat $\chi(a)$ volledig bepaald wordt door de karakterwaarde s op $\mathbb{F}_p^*$ en de waardes van $\chi(1 + x^i)$. We zullen aannemen dat $\chi$ niet-triviaal is op de verzameling $1 + (X^{n-1})$. Immers, als dit wel zo zou zijn, dan heeft de Gauss-som de waarde 0 (zie vorig hoofdstuk). Omdat $a \in A^*$ precies als de constante coëfficiënt 0 is, onderzoeken we de som:

$$\tau(\chi, \psi_b) = \sum_{\substack{a_0 \in \mathbb{F}_p^* \\ a_1 \in \mathbb{F}_p, \ldots, a_{n-1} \in \mathbb{F}_p}} \chi(a_0 + a_1X + ... + a_{n-1}X^{n-1})\psi_b(a_0 + a_1X + ... + a_{n-1}X^{n-1}) \tag{5.8}$$

Waarin $\psi_b = e(res(ba)), b \in A^*$. We kunnen opmerken dat het voldoende is om deze som te berekenen voor $b = 1$. Er geldt immers:

$$\tau(\chi, \psi_b) = \overline{\chi(b)}\tau(\chi, \psi_1). \tag{5.9}$$

Verder zien we dat $\psi_1(a_0 + a_1X + ... + a_{n-1}X^{n-1}) = e(a_{n-1})$. Laat $\widetilde{\tau}(\chi)$ de standaard Gauss-som zijn op $\mathbb{F}_p$, dan vinden we:

$$\begin{aligned}\tau(\chi, \psi_1) =& \sum_{\substack{a_0 \in \mathbb{F}_p^* \\ a_1 \in \mathbb{F}_p, \ldots, a_{n-1} \in \mathbb{F}_p}} \chi(a_0 + a_1X + ... + a_{n-1}X^{n-1})e(a_{n-1}) \\ =& \sum_{\substack{a_0 \in \mathbb{F}_p^* \\ \widetilde{a}_1 \in \mathbb{F}_p, \ldots, \widetilde{a}_{n-1} \in \mathbb{F}_p}} \chi(a_0)\chi(1 + \widetilde{a}_1X + ... + \widetilde{a}_{n-1}X^{n-1})e(a_0\widetilde{a}_{n-1}) \\ =& \sum_{\widetilde{a}_1 \in \mathbb{F}_p, \ldots, \widetilde{a}_{n-1} \in \mathbb{F}_p} \chi(1 + \widetilde{a}_1X + ... + \widetilde{a}_{n-1}X^{n-1}) \sum_{a_0 \in \mathbb{F}_p^*} \chi(a_0)e(a_0\widetilde{a}_{n-1}) \\ =& \sum_{\widetilde{a}_1 \in \mathbb{F}_p, \ldots, \widetilde{a}_{n-1} \in \mathbb{F}_p} \chi(1 + \widetilde{a}_1X + ... + \widetilde{a}_{n-1}X^{n-1})\overline{\chi(\widetilde{a}_{n-1})} \cdot \widetilde{\tau}(\chi)\end{aligned} \tag{5.10}$$

Het is dus voldoende om de som (5.10) te bepalen.

Omdat $p \geq n$, volgt dat $\chi(1+X^i)^p = 1$, dus $\chi(1+X^i) = e(b_i)$ voor zekere $b_i \in \mathbb{F}_p$. Omdat $\chi$ niet-triviaal is op $\chi(1+(X^{n-1})$, moet volgen dat $\chi(1+X^{n-1}) = e(b_{n-1})$ voor een zekere $b_{n-1} \in \mathbb{F}_p^*$. Het volgende lemma is nu van belang:

**Lemma 5.2.1.** *Laat $a = 1 + a_1X + ... + a_{n-1}X^{n-1} \in \mathbb{F}_p[X]/(X^n)$, met $p \geq n$. Dan bestaan er unieke $c_1, ..., c_{n-1} \in \mathbb{F}_p$ zodat*

$$a = (1+X)^{c_1} \cdot ... \cdot (1+X^{n-1})^{c_{n-1}} \tag{5.11}$$

*Bewijs.* We bewijzen dit met behulp van inductie naar $m$ in $\mathbb{F}_p[X]/(X^m)$. Merk op dat voor $m = 2$ geldt dat $a = 1 + a_1X = (1+X)^{a_1}$, dit geeft dus een unieke $c_1$. Stel dat de bewering juist is voor $m = k < n$. Laat $a \in \mathbb{F}_p[X]/(X^{k+1})$, dan bestaan er $c_1, ..., c_{k-1}$ zodat $a$ mod $X^k$ te schrijven is als:

$$a \equiv (1+X)^{c_1} \cdot ... \cdot (1+X^{k-1})^{c_{k-1}}$$

Er volgt dat er een $t \in \mathbb{F}_p$ bestaat zodat $a$ te schrijven is als:

$$\begin{aligned} a &= (1+X)^{c_1} \cdot ... \cdot (1+X^{k-1})^{c_{k-1}} + tX^k \\ &= (1+X)^{c_1} \cdot ... \cdot (1+X^{k-1})^{c_{k-1}} \cdot (1+X^k)^t \end{aligned}$$

Stel nu $(1+X)^{c_1} \cdot ... \cdot (1+X^{k-1})^{c_{k-1}} \cdot (1+X^k)^{c_k} = (1+X)^{c_1'} \cdot ... \cdot (1+X^{k-1})^{c_{k-1}'} \cdot (1+X^k)^{c_k'}$. Dan volgt door uniciteit mod $X^k$ dat $c_1 = c_1', ..., c_{k-1} = c_{k-1}'$. Uiteraard moet dan ook volgen $c_k = c_k'$. □

Met behulp van dit lemma volgt dat de som (5.10) gelijk is aan

$$S(\chi) = \sum_{\substack{c_1,...,c_{n-1} \in \mathbb{F}_p \\ \widetilde{a}_{n-1} \neq 0}} \chi(1+X)^{c_1} \cdot ... \chi(1+X^{n-1})^{c_{n-1}} \overline{\chi(\widetilde{a}_{n-1})}. \tag{5.12}$$

Door de termen $(1+X)^{c_1} \cdot ... \cdot (1+X^{n-1})^{c_{n-1}}$ uit te werken, is in te zien dat $\widetilde{a}_{n-1} - c_{n-1}$ niet de variabele $c_{n-1}$ bevat. We schrijven dus:

$$\begin{aligned} S(\chi) &= \sum_{c_1,...,c_{n-2} \in \mathbb{F}_p} \chi(1+X)^{c_1} \cdot ... \cdot \chi(1+X^{n-2})^{c_{n-2}} \sum_{\substack{c_{n-1} \in \mathbb{F}_p \\ \widetilde{a}_{n-1} \neq 0}} \chi(1+X^{n-1})^{c_{n-1}} \overline{\chi(\widetilde{a}_{n-1})} \\ &= \sum_{c_1,...,c_{n-2} \in \mathbb{F}_p} \chi(1+X)^{c_1} \cdot ... \cdot \chi(1+X^{n-2})^{c_{n-2}} \cdot \chi(1+X^{n-1})^{c_{n-1} - \widetilde{a}_{n-1}} \\ &\quad \cdot \sum_{u \in \mathbb{F}_p^*} \chi(1+X^{n-1})^u \overline{\chi(u)}. \end{aligned}$$

Merk op dat geldt $\sum_{u \in \mathbb{F}_p^*} e(b_{n-1}u)\overline{\chi(u)} = \overline{\sum_{u \in \mathbb{F}_p^*} e(-b_{n-1}u)\chi(u)} = \chi(-b_{n-1})\overline{\widetilde{\tau}(\chi)}$. Er geldt nu dus:

$$\tau(\chi, \psi_1) = p \cdot \chi(-b_{n-1}) \left( \sum_{c_1,...,c_{n-2} \in \mathbb{F}_p} \chi(1+X)^{c_1} \cdot ... \cdot \chi(1+X^{n-2})^{c_{n-2}} \cdot \chi(1+X^{n-1})^{c_{n-1} - \widetilde{a}_{n-1}} \right) \tag{5.13}$$

In de volgende paragrafen zullen we (5.13) berekenen voor een aantal waarden voor $n$. We zullen hiervoor de kwadratische Gauss-sommen uit paragraaf 5.1 nodig hebben. Uiteraard is dit niet algemeen, maar we kunnen inzien dat in het algemeen wel iets soortgelijks blijft gelden. Voor even $n$ zal de algemene gedaante van de Gauss-som $e(t)p^{0.5n}\chi(-b_{n-1})$ zijn, waar t een functie is van $b_1, ..., b_{n-1}$. Voor oneven $n$ zal de som altijd van de vorm $(\frac{-2^{-1}b_{n-1}}{p})e(t)p^{0.5n+0.5}\chi(-b_{n-1})i^{\frac{(p-1)^2}{4}}$ zijn, omdat voor oneven $n$ de kwadratische Gauss-som moet worden berekend.

### 5.2.1 Gauss-sommen op $\mathbb{F}_p[X]/(X^2)$

Met behulp van de som (5.10) kunnen we de Gauss-som op $\mathbb{F}_p[X]/(X^2)$ berekenen. Dit betekent dat we de som

$$\widetilde{\tau}(\chi)\sum_{\widetilde{a}_1\in\mathbb{F}_p}\chi(1+\widetilde{a}_1)\overline{\chi(\widetilde{a}_1)}$$

moeten berekenen. We kunnen dit relatief eenvoudig berekenen.

$$\begin{aligned}\sum_{\widetilde{a}_1\in\mathbb{F}_p}\chi(1+\widetilde{a}_1)\overline{\chi(\widetilde{a}_1)} &= \sum_{\widetilde{a}_1\in\mathbb{F}_p} e(b_1\widetilde{a}_1)\overline{\chi(\widetilde{a}_1)}\\ &= \overline{\sum_{\widetilde{a}_1\in\mathbb{F}_p} e(-b_1\widetilde{a}_1)\chi(\widetilde{a}_1)}\\ &= \chi(-b_1)\overline{\widetilde{\tau}(\chi)}\end{aligned}$$

We vinden nu dus:

$$\tau(\chi,\psi_1) = \chi(-b_1)p \tag{5.14}$$

### 5.2.2 Gauss-sommen op $\mathbb{F}_p[X]/(X^3)$

We gaan nu de Gauss-som op $\mathbb{F}_p[X]/(X^3)$ met $p \geq 3$. We moeten de coëfficiënt $\widetilde{a}_2$ nu berekenen in termen van $c_1$ en $c_2$. Met het binomium van Newton vinden we:

$$(1+X)^{c_1}(1+X^2)^{c_2} = \left(\sum_{k=0}^{n-1}\binom{c_1}{k}X^k\right)\left(\sum_{k=0}^{n-1}\binom{c_2}{k}X^{2k}\right)$$

Er geldt nu $\widetilde{a}_2 = \binom{c_1}{2} + c_2$. Gebruikmakend van (5.13) berekenen we het volgende:

$$\begin{aligned}\sum_{c_1\in\mathbb{F}_p}\chi(1+X)^{c_1}\chi(1+X^2)^{-\binom{c_1}{2}} &= \sum_{c_1\in\mathbb{F}_p} e(b_1c_1)e(-b_2\binom{c_1}{2})\\ &= \sum_{c_1\in\mathbb{F}_p} e(-2^{-1}b_2c_1^2 + c_1(-2^{-1}b_2+b_1))\end{aligned}$$

Deze laatste som is een kwadratische Gauss-som, en deze kunnen we daarom met behulp van lemma 5.1.4 uitrekenen. We zien dus dat de waarde van deze Gauss-som gelijk is aan:

$$\tau(\chi,\psi_1)=\left(\frac{-2^{-1}b_2}{p}\right)e(2^{-1}(b_1+2^{-1}b_2)^2b_2^{-1})\chi(-b_2)p^{1.5}i^{\frac{(p-1)^2}{4}} \tag{5.15}$$

### 5.2.3 Gauss-sommen op $\mathbb{F}_p[X]/(X^4)$

Nu gaan we de Gauss-som op $\mathbb{F}_p[X]/(X^4)$ berekenen met $p \geq 4$. Wederom moeten we de coëfficiënt $\widetilde{a}_3$ bepalen in termen van $c_1$,$c_2$ en $c_3$. Met het binomium van Newton vinden we:

$$(1+X)^{c_1}(1+X^2)^{c_2}(1+X^3)=\left(\sum_{k=0}^{n-1}\binom{c_1}{k}X^k\right)\left(\sum_{k=0}^{n-1}\binom{c_2}{k}X^{2k}\right)\left(\sum_{k=0}^{n-1}\binom{c_3}{k}X^{3k}\right)$$

Er geldt nu $\widetilde{a}_3=\binom{c_1}{3}+c_1c_2+c_3$. Gebruikmakend van (5.13) berekenen we het volgende:

$$\sum_{c_1,c_2\in\mathbb{F}_p}\chi(1+X)^{c_1}\chi(1+X^2)^{c_2}\chi(1+X^3)^{-(\binom{c_1}{3}+c_1c_2)}=$$

$$\sum_{c_1,c_2\in\mathbb{F}_p}e(b_1c_1)e(b_2c_2)e(-b_3(\binom{c_1}{3}+c_1c_2))$$

Dit geeft nu de volgende dubbele som:

$$\sum_{c_1\in\mathbb{F}_p}e(b_1c_1-b_3\binom{c_1}{3})\sum_{c_2\in\mathbb{F}_p}e(c_2(b_2-b_3c_1))$$

De binnenste som is een meetkundige reeks en heeft de waarde $p$ als $b_2=b_3c_1$ en 0 anders. Als we voor $c_2$ $b_2b_3^{-1}$ invullen vinden we nu de volgende waarde voor de Gauss-som:

$$\tau(\chi,\psi_1)=e(b_1b_2b_3^{-1}-6^{-1}b_2(b_2b_3^{-1}-1)(b_2b_3^{-1}-2))p^2\chi(-b_3) \tag{5.16}$$

# Hoofdstuk 6

# Conclusie en discussie

Door een algemene uitdrukking voor het additieve karakter op de algebra $A = \mathbb{F}_q[X]/(f(X)^n)$, te vinden met behulp van het residu van een element $a \in A$ (zoals gedefinieerd door [6]), kan de modulus van de Gauss-som bepaald worden. De modulus bleek voor additieve karakters van de vorm $\psi_v$ met $v \in A^*$ gelijk te zijn aan $\sqrt{|A|}$ (onder bepaalde aannames van de trivialiteit van het multiplicatieve karakter).
Verder probeerden we een uitdrukking te vinden voor het argument van de Gauss-som. Dit is gelukt voor de algebra $\mathbb{F}_p[X]/(X^n)$, met $n \geq p$ voor $n = 2, 3$ en 4. Hoewel we een goed beeld hebben van hoe de Gauss-som er op deze algebra er uitziet, blijft het lastig om er een expliciete formule voor te geven. Om een expliciete uitdrukking te geven moeten we een algemene uitdrukking vinden voor de coëfficiënt van $X^{n-1}$ in termen van $c_1, c_2, ..., c_{n-1}$ in de uitdrukking:

$$(1 + X)^{c_1} \cdot (1 + X^2)^{c_2} \cdot ... \cdot (1 + X^{n-1})^{c_{n-1}}.$$

Uiteraard kan ook nog naar het argument van de Gauss-som op de algebra $\mathbb{F}_q[X]/(f(X)^n)$ gekeken worden. Op deze algebra kan alleen niet een vergelijkbare ontbinding worden gemaakt als bij de algebra $\mathbb{F}_p[X]/(X^n)$.

# Bibliografie


[1] F. Beukers. *Elementary Numbertheory.* Universiteit Utrecht. Utrecht, 2012.

[2] F. Beukers. *Rings and Galoistheory.* Universiteit Utrecht. Utrecht, 2016.

[3] H. Cohen. *Number Theory, Volume I: Tools and Diophantine Equations.* Springer, New York, 2007.

[4] S. Ghorpade. *Notes on Galoistheory.* Department of Mathematics, Indian Institute of Technology, Bombay, 1994.

[5] K. Ireland and M. Rosen. *A Classical Introduction to Modern Number Theory.* Springer, New York, 1982.

[6] T. Nan and C. Hsu. *On Polynomial Gauss sums mod* $P^n, n \geq 2$. *Acta Arithmetica*, 143:393–401, 2010.