Oplosbaarheid in radicalen in polynomiale tijd

Rens de Heer

Januari 2017

1 Inleiding

Sinds de tijd van de Babyloniërs zijn wiskundigen bezig om oplossingen te vinden voor simpelste vorm van vergelijkingen, de polynoomvergelijkingen. De Babyloniërs slaagden erin om de oplossingen van een kwadratische vergelijking te vinden met een algemene formule [1]. Sindsdien hebben veel wiskundigen geprobeerd om de 3e graadsvergelijking op te lossen met een algemene formule, dit lukte Cardano in zijn "Ars Magna". Daarmee was ook meteen de 4e graadsvergelijking opgelost omdat er al een oplossing lag die de 3e graadsvergelijking gebruikte. De jaren daarna zijn veel wiskundigen bezig geweest om een algemene formule te vinden van de 5e graadsvergelijking. Abel bewees in 1823 [2] dat de oplossing van een algemene 5^e graadsvergelijking niet geschreven kan worden in radicalen (combinaties van n-de graadswortels en getallen in $\mathbb{Q}$). Er is dus geen algemene formule.

Een paar jaar later schreef de jonge wiskundige Galois, op de vooravond van zijn dood, alles wat hij wist over polynomen, waaronder een bewijs voor dezelfde stelling. Dit deed hij zonder kennis te nemen van het bewijs van Abel. Abel gebruikte in zijn bewijs de eigenschappen van permutaties in S_5, maar Galois ging een stap verder en ontwikkelde een hele theorie over hoe groepen en polynomen zich tot elkaar verhouden. Dit noemen we nu Galoistheorie. Hiermee gaf Galois ook een criterium voor welke polynomen met graad > 4 wel oplosbaar zijn in radicalen.

Niet elke concrete n-de graadsvergelijking ($n \geq 5$) is onmogelijk om op te lossen in radicalen, bijvoorbeeld $n^5 = 2$ heeft natuurlijk als oplossing $\sqrt[5]{2}$. Om te bepalen of een polynoom oplosbaar is in radicalen moet men eerst de galoisgroep vinden en dan bepalen of deze groep de (niet zo toevallig gekozen) eigenschap "oplosbaar" heeft. Het vinden van deze groep kan erg lang duren als de polynoom een hoge graad heeft. Er bestaat tot op heden nog geen algoritme om dit in polynomiale tijd (in de graad van $f(x)$) te doen.

In deze scriptie wordt er gebruikt gemaakt van de eigenschappen van bepaalde groepen om de volgende eigenschap te bepalen van polynomen: **"Is een polynoom $f(x)$ met gehele coëfficiënten oplosbaar in radicalen?"**

Er zal niet alleen aandacht besteed worden aan het vinden van het antwoord, maar dit zal ook in polynomiale tijd gebeuren in de graad van $f(x)$. De scriptie is gebaseerd op het werk van Landau en Miller [9].

Hiervoor wordt gebruikt gemaakt van een eigenschap van transitieve groepsacties genaamd de "Imprimitieve blokken". Deze zullen van pas komen tijdens het maken van een speciale toren van lichaamsuitbreidingen tussen een wortellichaam $\mathbb{Q}(\alpha)$ van $f(x)$ en $\mathbb{Q}$. Met deze toren veranderen we de vraag of een polynoom een oplosbare galoisgroep heeft naar meerdere vragen ($log(deg(f))$) of elke tussenliggende uitbreiding een oplosbare galoisgroep heeft. Deze uitbreidingen zijn zo gemaakt dat ze allemaal een primitieve galoisgroep hebben. En een primitieve oplosbare groep is polynomiaal gelimiteerd in orde [11]. Hierdoor kunnen we sneller bepalen of de galoisgroep oposbaar is.

2 Basistheorie en stellingen

2.1 Lichaamstheorie

Lichamen zijn het belangrijkste stuk theorie om polynomen beter te begrijpen. Ik zal nu even een paar belangrijke definities en stellingen ophalen. Deze zijn ook allemaal te vinden in [5].

Lichamen: Een lichaam is een ring waarin vermenigvuldigen commutatief is en waarin elk element ongelijk aan 0 een inverse heeft. De verzameling $\mathbb{Q}$ met de gebruikelijke optelling en vermenigvuldiging is bijvoorbeeld een lichaam. Het is zelfs het kleinste oneindige lichaam [5].

Lichaamsuitbreiding: Intuïtief is een lichaamsuitbreiding $K(\alpha)$ van een lichaam K het kleinste lichaam wat K en α bevat. Bijvoorbeeld: $\mathbb{Q}(\sqrt[3]{2})$. Dit lichaam bestaat uit alle getallen in de vorm $a+b\sqrt[3]{2}+c\sqrt[3]{2}^2$. Vaak wordt er in plaats van een element toevoegen gewerkt met de minimaalpolynoom van een element: $\mathbb{Q}[x]/(f(x))$. Dit lichaam is isomorf aan het lichaam $\mathbb{Q}(\alpha)$, waar α een wortel is van $f(x)$. In het geval van $\alpha = \sqrt[3]{2}$ is de minimaalpolynoom $x^3 - 2 = 0$. Let erop dat de notatie $\mathbb{Q}[x]/(x^3-2)$ niet genoeg is om het lichaam goed aan te wijzen, de minimaalpolynoom heeft namelijk meerdere wortels die in dit geval bijvoorbeeld een ander lichaam definiëren. Het is wel zo dat al deze lichamen isomorf aan elkaar zijn.

Irreducibel: Een polynoom heet irreducibel over een lichaam als deze niet is op te splitsen in een product van polynomen van lagere graad. Bijvoorbeeld $x^2 + 2x + 1$ is niet irreducibel over $\mathbb{Q}$ omdat $x^2 + 2x + 1 = (x + 1)(x + 1)$, maar $x^2 - 2$ is wel irreducibel over $\mathbb{Q}$.

Splijtlichaam: Als we een lichaam K uitbreiden met alle wortels van $f(x) \in K[x]$ in een algebraïsch afgesloten lichaam, dan spreken we over het splijtlichaam van $f(x)$ over K. Als we werken in $\mathbb{Q}$, kunnen we $\mathbb{C}$ gebruiken als algebraïsch afgesloten lichaam. Bijvoorbeeld het splijtlichaam van $x^3 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[3]{2}, \frac{1}{2} + \frac{i\sqrt{3}}{2})$.

Normale/Galoisuitbreiding: Als een lichaamsuitbreiding een splijtlichaam is van een polynoom over het basislichaam spreken van een normale uitbreiding. Een uitbreiding van graad 2 is altijd normaal, omdat als de ene wortel $a + b\sqrt{c}$ in een lichaam zit, zit de andere wortel $a - b\sqrt{c}$ ook in dat lichaam. Maar het de uitbreiding $\mathbb{Q}(\sqrt[3]{2})$ is geen normale uitbreiding omdat niet alle wortels van x^3-2 in dit lichaam zitten. Een Galoisuitbreiding is een normale en "seperable" uitbreiding. In het geval van uitbreidingen over $\mathbb{Q}$ geldt dit laatste automatisch.

Primitief element: Een lichaamsuitbreiding kan gemaakt worden door meerdere elementen toe te voegen aan het basislichaam. Als een lichaam uitgebreid is met 1 element, dan heet dit element een primitief element voor deze uitbreiding. We weten dat elke eindige uitbreiding van $\mathbb{Q}$ te schrijven als een uitbreiding met 1 element [13]. De uitbreiding $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is bijvoorbeeld ook te schrijven als $\mathbb{Q}(\sqrt{2} + \sqrt{3})$. In het algoritme komt het vaker voor dat we een primitief element construeren.

Galoisgroep: De Galoisgroep van een galoisuitbreiding is verzameling van automorphismen over het nieuwe lichaam, die het oude lichaam fixeren. De galoisgroep van bijvoorbeeld: $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is de verzameling: $\{e, (\sqrt{2} \mapsto -\sqrt{2})\} \cong \mathbb{Z}_2$. Als we de galoisgroep van een polynoom $f(x) \in K[x]$ zeggen, bedoelen we de galoisgroep van het splijtlichaam van $f(x)$ over het K.

2.2 Galoistheorie

Zoals in de inleiding genoemd is, is er een één op één relatie tussen ondergroepen van de galoisgroep van een galoisuitbreiding en de tussenliggende deellichamen. Formeel gezegd bestaat dit uit de volgende stellingen:

Stelling 2.1 (Hoofdstelling van de Galoistheorie)**.** *Laat K een lichaam zijn en $f(x)$ een irreducibel polynoom in $K[x]$ met wortels $\alpha_1, ..., \alpha_m$, dan:[5]*

- *Elk lichaam $K(\beta)$ tussen K en het splijtlichaam $K(\alpha_1, ..., \alpha_m)$ van $f(x)$ definieert een ondergroep H van de galoisgroep G, namelijk de groep van autormorphismen die $K(\beta)$ fixeren.*
- *Elke subgroep H definieert een deellichaam $K(\beta)$, namelijk de elementen uit $K(\alpha_1, ..., \alpha_m)$ die gefixeerd zijn door H.*

- *De orde van G is gelijk aan de graad van $K(\alpha_1, ..., \alpha_m)/K$. En de orde van H is gelijk aan de graad van $K(\alpha_1, ..., \alpha_m)/K(\beta)$.*
- *De ondergroep H is normaal dan en slechts dan als $K(\alpha_1, ..., \alpha_m)$ over $K(\beta)$ is een Galoisuitbreiding. De galoisgroep van $K(\beta)$ over K is dan G/H*

Deze stellingen beschrijft de correspondentie van lichamen en groepen. Op deze manier kan men bepaalde dingen bewijzen over polynomen door iets te bewijzen over groepen. En andersom. Een voorbeeld van het gebruik van deze correspondentie is het criterium voor de oplosbaarheid van een polynoom in radicalen.

2.3 Radicalen en oplosbare groepen

Zoals in de inleiding genoemd, is een radicaal een getal wat geschreven kan worden door rationele getallen te combineren met n-de graadswortels. Deze beschrijving kunnen we formeel opschrijven: Een radicaal is een getal dat voorkomt in een eindige toren van lichaamsuitbreidingen over K, waarbij elke uitbreiding een wortel van $x^n - a$ toevoegt, waarbij a een element is in het vorige lichaam. Al deze uitbreidingen zijn normaal en hebben een cyclische galoisgroep [5]. Dat betekent dat de volledige galoisgroep een eindige reeks van normale ondergroepen heeft, waarin elk quotiënt van twee opeenvolgende groepen een cyclische groep is. Een groep met deze eigenschap heet een **oplosbare groep**.

Stelling 2.2 (Hoofdstelling van oplosbaarheid in radicalen)**.** *Alle wortels van een polynoom $f(x) \in K[x]$ is te schrijven in radicalen over K dan en slechts dan als de galoisgroep van $f(x)$ over K een oplosbare groep is [5].*

We kunnen in plaats van naar de gehele lichaamsuitbreiding te kijken, ook kijken naar tussenliggende uitbreidingen:

Lemma 2.3. *Stel $K \subset K(\beta) \subset K(\alpha)$. Dan is elk element uit $K(\alpha)$ te schrijven in radicalen over K, dan en slechts dan als elk element te schrijven is in radicalen over $K(\beta)$ en elk element uit $K(\beta)$ te schrijven is in radicalen over K.*

Bewijs: Als elk element uit $K(\beta)$ te schrijven is in radicalen over K, dan is er een eindige toren van (radicale) lichaamsuitbreidingen tussen $K(\beta)$ en K. En als elk element uit $K(\alpha)$ te schrijven in radicalen over $K(\beta)$, dan is er een eindige toren van (radicale) lichaamsuitbreidingen tussen $K(\alpha)$ en $K(\beta)$. Als we deze twee torens achter elkaar zetten, is er een toren tussen $K(\alpha)$ en K en is elke element uit $K(\alpha)$ te schrijven in radicalen over K.

Als elk element in $K(\alpha)$ geschreven kan worden in radicalen over K, dan kan natuurlijk ook geschreven worden in radicalen over $K(\beta)$ en kan ook elk element van $K(\beta)(\subset K(\alpha))$ geschreven worden in radicalen over K. □

Dit betekent dat wanneer we een toren van lichaamsuitbreidingen $K \subset K(\alpha_1) \subset ... \subset K(\alpha_k) = Splijtlichaam(f(x))$ hebben gemaakt, we naar elke tussenliggende uitbreiding $K(\alpha_{i+1})/K(\alpha)$ kunnen kijken. Elk element uit $K(\alpha_{i+1})$ kan geschreven worden in radicalen over $K(\alpha)$ voor alle i, dan en slechts dan als $f(x)$ oplosbaar is in radicalen.

Een handige manier om te bepalen of een groep oplosbaar is, is te kijken naar de commutator reeks. Deze is als volgt gedefinieerd:

- $G^0 = G$
- $G^n = [G^{n-1}, G^{n-1}]$

Hierbij is $[G^{n-1}, G^{n-1}]$ de groep voortgebracht door de commutators $(ghg^{-1}h^{-1})$ van G^{n-1}.

Lemma 2.4. *Een groep G is oplosbaar dan en slechts dan als de commutator reeks termineert tot de triviale groep $\{e\}$ [6].*

Deze eigenschap wordt gebruikt in sectie 5.5.

3 Groepacties

De galoisgroep van een (irreducibel) polynoom heeft een groepsactie die transitief werkt op de wortels van de polynoom [12]. Bij het algoritme gaan we een bepaalde eigenschap gebruiken van deze groepsactie. De zogenaamde imprimitieve blokken. Dit zijn speciale deelverzamelingen waar de groep op werkt. Deze blokken worden namelijk als een geheel gepermuteerd door een groepsactie. Ze hangen nauw samen met de stabilisator van een element. In dit hoofdstuk noemen we de groep G en de verzameling waar de groep op werkt X. Ook werkt G altijd transitief op X.

3.1 Stabilisator

De **stabilisator** van een element α uit X is de deelverzameling van G die α op zichzelf afbeeldt.

$$G_\alpha = \{\sigma \in G : \sigma(\alpha) = \alpha\}$$

Deze verzameling vormt een ondergroep van G. We kunnen ook de stabilisator van een deelverzameling definiëren:

$$G_\Lambda = \{\sigma \in G : \sigma(\Lambda) = \Lambda\}$$

Het betekent niet dat alle elementen van Λ puntsgewijs worden vastgezet. Deze verzameling vormt ook een ondergroep.

We weten uit volgens de baan-stabilisatorstelling dat:

$$|Baan(\alpha)| = |G|/|G_\alpha|$$

We weten uit de hoofdstelling van de Galoistheorie dat een ondergroep van G correspondeert met een deellichaam van het splijtlichaam van $f(x)$. Dit deellichaam wordt gefixeerd door de ondergroep. Het lichaam wat correspondeert met G_α is dus $\mathbb{Q}(\alpha)$ (waarbij α een wortel is van $f(x)$). Het deellichaam wat correspondeert met G_Λ is het lichaam gegenereerd door de symmetrische functies van $\{\alpha_1, ..., \alpha_k\} = \Lambda$. Deze functies blijven namelijk hetzelfde na elke willekeurige permutatie van G die Λ op zichzelf afbeeldt.

3.2 Imprimitieve blokken

Een blok B is een deelverzameling van X, die na elke groepsactie volledig wordt afgebeeld op B of volledig niet op B:

$$B \text{ is een blok als: } \sigma B \cap B = B \textbf{ of } \sigma B \cap B = \varnothing.(\forall \sigma \in G)$$

B wordt een **imprimitief blok** genoemd als B niet triviaal is: $B \neq \{\alpha\}$ en $B \neq X$. Als B een blok is, zijn $\sigma_1 B, ..., \sigma_i B$ ook allemaal een blok. Deze blokken samen worden een **compleet blok systeem** genoemd. Deze blokken vormen een partitie van X. Een imprimitief blok met minimaal aantal elementen wordt een **minimaal imprimitief blok** genoemd.

Voordat we de twee belangrijke stellingen gaan behandelen, merken we eerst het volgende lemma op:

Lemma 3.1. *Als B een blok is dat α bevat, dan is $G_\alpha < G_B$.*

Bewijs: neem $\sigma \in G_\alpha$, dan is $\sigma(\alpha) = \alpha$. Dus $\sigma(B) \cap B \neq \varnothing$. B is een blok dus $\sigma(B) = B$ en dus $\sigma \in G_B$.□

In paragraaf 5.3 gaan we een minimaal imprimitief blok maken aan de hand van de volgende 2 stellingen.

Stelling 3.2. *Alle punten die worden vastgezet door G_α vormen een blok:*

$$\Lambda = \{\beta : \forall \sigma \in G_\alpha, \sigma(\beta) = \beta\} \implies \Lambda \textit{ is een blok}$$

Bewijs: Neem $\beta \in \Lambda$. Dat betekent dat $\sigma \in G_\alpha \implies \sigma \in G_\beta$. Maar omdat G transitief werkt, is de baan van α en die van β gelijk aan de gehele verzameling. En dan volgt uit $|baan(\beta)| = |baan(\alpha)| = |G|/|G_\alpha| = |G|/|G_\beta|$, dat de orde van G_α gelijk is aan G_β en dus $G_\alpha = G_\beta$. Neem nu aan dat $\sigma\Lambda \cap \Lambda$ niet leeg is, en kies $\beta \in \sigma\Lambda \cap \Lambda$. Dan is $\beta = \sigma(\gamma)$ voor $\gamma \in \Lambda$. En $\tau(\beta) = \beta$ voor $\tau \in G_\alpha$. Neem nu $\sigma\tau\sigma^{-1}(\beta) = \sigma\tau(\gamma) = \sigma(\gamma) = \beta$. Dus $\sigma\tau\sigma^{-1} \in G_\beta = G_\alpha$. Neem nu $\rho \in \Lambda$, dan $\sigma\tau\sigma^{-1}(\rho) = \rho$, dus $\tau\sigma^{-1}(\rho) = \sigma^{-1}(\rho)$ voor alle $\tau \in G_\alpha$. Dus $\sigma^{-1}(\rho)$ is een element van Λ. Dus $\sigma^{-1}(\Lambda) = \Lambda$ voor alle $\sigma \in G$. Dus Λ is een blok. □

Stelling 3.3. *Als er naast α geen andere punten worden vastgezet door G_α en Λ is een minimaal imprimitief blok, dan geldt: $\forall\gamma \in \Lambda$ met $\gamma \neq \alpha$ dan is dit blok gelijk aan: $\Lambda = \{\sigma(\alpha)|\sigma \in \langle G_\alpha, G_\gamma\rangle\}$ ($\langle G_\alpha, G_\gamma\rangle$ is de groep voortgebracht door G_α en G_γ)*

Bewijs: Neem $\gamma \in \Lambda, \gamma \neq \alpha$. Maak dan $\Delta = \{\sigma(\alpha)|\sigma \in \langle G_\alpha, G_\gamma\rangle\}$. Volgens lemma 3.1 weten we dat $G_\alpha < G_\Lambda$ en $G_\gamma < G_\Lambda$, dus $\langle G_\alpha, G_\gamma\rangle < G_\Lambda$, en daarom is $\Delta \subset \Lambda$. Neem aan dat $\Delta \cap \tau\Delta$ niet leeg is, en kies $\beta \in \Delta \cap \tau\Delta$. Dan $\beta = \sigma_1(\alpha)$ en $\beta = \tau\sigma_2(\alpha)$, voor σ_1 en σ_2 in $\langle G_\alpha, G_\gamma\rangle$. Dus $\sigma_1(\alpha) = \tau\sigma_2(\alpha)$ geeft $\alpha = \sigma_1^{-1}\tau\sigma_2(\alpha)$. Dus $\sigma_1^{-1}\tau\sigma_2$ is een element van G_α. Dus moet τ ook een element zijn van $\langle G_\alpha, G_\gamma\rangle$. En dus $\tau\Delta = \Delta$. Dus Δ is een blok. Maar Λ is een minimaal imprimitief blok dat α bevat, dus $\Delta = \Lambda$. □

4 Gereedschappen

4.1 Norm

Een belangrijke techniek in het factoriseren van polynomen is de Norm van een element over een uitbreiding: $N_{E/F}(\beta)$. Deze is als volgt gedefinieerd: De norm van $\beta = a_0 + a_1\alpha + ... + a_{m-1}\alpha^{m-1} \in K(\alpha)$ is:

$$N_{K(\alpha)/K}(\beta) = \Pi_i(a_0 + a_1\alpha_i + ... + a_{m-1}\alpha_i^{m-1})$$

Waarbij α_i de geconjugeerden van $\alpha = \alpha_1$ zijn. Deze definitie kunnen we ook gebruiken om de norm van een polynoom te definiëren. Als we in polynoom $f_\alpha(x)$ in $\mathbb{Q}(\alpha)[x]$ hebben, dan is de norm

$$N(f_\alpha(x))) = \Pi_i(f_{\alpha_i}(x))$$

Deze norm is een polynoom in $\mathbb{Q}[x]$.

4.2 Factoriseren

Lenstra, Lenstra en Lovász [10] hebben een algoritme ontwikkeld wat een polynoom in $\mathbb{Q}[x]$ kan factoriseren in polynomiale tijd. Landau [8] heeft dit algoritme uitgebreid om een polynoom in $\mathbb{Q}(\alpha)[x]$ te factoriseren ($f(\alpha) = 0$). Dit kan door de eerst de norm te nemen van de polynoom $f(x)$, die factoriseren over $\mathbb{Q}[x]$ en dan die factorisatie terug brengen naar de oorspronkelijke polynoom door de grootste gemeenschappelijke deler te nemen van elke factor in $N(f(x))$ en $f(x)$. over $Q[\alpha]/f(\alpha)$.

Om een polynoom te factoriseren in $\mathbb{Q}(\alpha_1, \alpha_2)$, gebruikt Landau de factorisatie over $\mathbb{Q}(\alpha)[x]$ om een primitief element β te vinden voor $\mathbb{Q}(\alpha_1, \alpha_2)$. En dan kan de factorisatie gemakkelijk omgeschreven worden naar $\mathbb{Q}(\beta)$ [8].

Deze laatste techniek wordt gebruikt in 5.1 en in 5.3.

4.3 Primitief element maken

We weten dat elke eindige uitbreiding van $\mathbb{Q}$ te schrijven is als een uitbreiding met 1 element. Er zijn namelijk maar eindig veel $c \in \mathbb{Z}$ waarvoor $\mathbb{Q}(\alpha + c\beta)$ niet gelijk is aan het lichaam $\mathbb{Q}(\alpha, \beta)$. Volgens Yokoyama, Noro en Takeshima [13] is het aantal $c \in \mathbb{Z}$ maximaal $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$. Dit kunnen we gebruiken om een primitief element te vinden voor een uitbreiding. Om te controleren of een

element een primitief element is, moeten we een lineair onafhankelijkheidsprobleem oplossen. Dit kan in polynomiale tijd gedaan worden volgens Edmonds [4].

Als we het primitieve element kunnen vinden voor een lichaam voortgebracht door 2 elementen kunnen we iteratief een primitief element voor een lichaam voortgebracht door n elementen.

4.4 Minimaalpolynoom maken

Tijdens het algoritme komt het voor dat we in een lichaam $\mathbb{Q}[z]/f(z)$ werken. In dit lichaam gaan we dan een primitief element $\beta(z)$ creëren voor een onderliggend lichaam. Als we dit gedaan hebben, willen we van dit element een minimaalpolynoom maken. Dit kunnen we doen op de volgende manier:

Zolang $\{1, \beta(z), \beta(z)^2, ..., \beta(z)^k\}$ een lineair onafhankelijke verzameling is, verhoog k met 1.

Wanneer dit algoritme termineert hebben we lineaire afhankelijke verzameling gevonden met een minimaal aantal elementen. De lineaire combinatie $\beta(z)^k + d_{n-1}\beta(z)^{k-1} + ... + d_0$ definieert dan een minimaalpolynoom $x^k + d_{n-1}x^{k-1} + ... + d_0$ voor $\beta(z)$. Dit is ook een lineair onafhankelijkheidsprobleem. En kan dus ook in polynomiale tijd.

5 Het algoritme

De naïeve manier om te bepalen of een polynoom oplosbaar is in radicalen, is door de galoisgroep te vinden en dan van deze groep te bepalen of deze oplosbaar is. Het vinden van de galoisgroep is op zichzelf al een niet triviale bezigheid. We beginnen met het behandelen van een algoritme voor dit probleem.

5.1 Galoisgroep vinden

Er zijn verschillende manieren om eigenschappen vast te stellen van de galoisgroep aan de hand van de polynoom. Zo kan je bijvoorbeeld de discriminant nemen en als deze een kwadraat is, is de galoisgroep een (onder)groep van A_n. Als je een lijst opstelt van alle transitieve subgroepen van S_n, en deze dan op een soortgelijke manier probeert te karakteriseren door de invarianten van het polynoom, dan is het voor kleine n < 10 mogelijk om de galoisgroep vast te stellen. Maar in het algemeen werkt dit niet.

Om in het algemeen de volledige groepstabel te vinden gebruiken we het algoritme wat Landau ontwikkeld heeft [7]. Dit algoritme voegt iteratief een wortel van een polynoom $f(x)$ toe aan $\mathbb{Q}$, totdat het splijtlichaam K is bereikt. Tijdens elke stap wordt het primitieve element voor het lichaam berekend en een minimaalpolynoom $g(x)$ voor dit element. Door $g(x)$ te vergelijken met $f(x)$ is de galoisgroep te vinden. Bekijk Algoritme 5.1.

$g(x)$ splijt over K omdat het een normale uitbreiding is. Elke wortel is dus te schrijven in termen van het primitieve element y:

$$g(x) = \prod_i^m (x - p_i(y))$$

$f(x)$ splijt ook over dit lichaam in de factoren:

$$f(x) = \prod_i^n (x - q_i(y))$$

Omdat het aantal elementen van de galoisgroep G gelijk is aan het aantal wortels van $g(x)$, is er precies 1 element σ_i uit G dat $p_1(y) = \gamma$ afbeeldt op $p_i(y)$. Zo weten we dus wat elk element uit de groep doet met het primitieve element. Deze actie kunnen we dan uitvoeren op de wortels van $f(x)$ en kijken hoe de galoisgroep werkt op $f(x)$. En zo komen we erachter welke ondergroep van S_n de galoisgroep is.

Om te kijken wat de galoisgroep doet met de wortels van $f(x)$, laten we elk element σ_i werken op de wortels van $f(x)$. Omdat we weten wat elk element σ_i doet met het primitieve element, is de actie

Algoritme 5.1 galoisgroep ($GALOIS$)

Input: $f(x) \in \mathbb{Q}[x]$ irreducibel met graad n
$m \leftarrow n$
Factoriseer $f(x)$ over $\mathbb{Q}[z]/(f(z))$:
$f(x) = \prod_i^k g_i(x)$
if Er is een $g_i(x)$ niet lineair met graad l **then**
    $m \leftarrow m * l$
    Vind het primitieve element γ' voor $\mathbb{Q}(\gamma)[y]/(g(y))$
    $\gamma \leftarrow \gamma'$
    Ga naar 2: en factoriseer over $\mathbb{Q}(\gamma)[x]$
end if
$g(x) = MinimaalPolynoom(\gamma)$
$f(x) = \prod_i^n (x - q_i(\gamma))$
$g(x) = \prod_i^m (x - p_i(\gamma))$ ▷ De wortels $q_i(\gamma)$ en $p_i(\gamma)$ zijn polynomen in het primitieve element.
for $i = 1, ..., n$ **do**
    for $j = 1, ..., m$ **do**
        $\tau_i(j) \leftarrow l$ Als $q_i(p_j(y)) = q_l(y)$ in $\mathbb{Q}[y]/g(y)$
    end for
end for
Return $\{\tau_i | i, ..., m\}$ ▷ De galoisgroep van $f(x)$.

op de wortels $q_i(\gamma)$ ook te bepalen. We laten eerst $p_i(y)$ op het primitieve element werken en daarna plaatsen we het resultaat in een wortel van $f(x)$:

We nemen dus $q_j(p_i(y))$ voor alle $i < m$ en $j < n$ over $K(y)/g(y)$. Dit worden andere wortels van $f(x)$, en zo weten we hoe de galoisgroep werkt op de wortels van $f(x)$, en dus welke ondergroep van S_n het is.

Er is alleen een probleem met dit algoritme. Er zijn galoisgroepen die zo groot kunnen worden dat ze niet meer polynomiaal in de graad van $f(x)$ zijn, bijvoorbeeld $|S_n| = n!$. Het vinden van de galoisgroep kost dan ook langer dan polynomiale tijd.

5.2 Volledig algoritme

Het algoritme van de vorige sectie werkt alleen maar in polynomiale tijd van de input als de galoisgroep polynomiaal in orde is. Dankzij Pálfy [11] weten we dat primitief oplosbare groepen polynomiaal gelimiteerd zijn in orde:

Stelling 5.1 (Pálfy)**.** *Als G een primitieve oplosbare groep is die transitief werkt op n elementen, dan* $|G| \leq 24^{-1/3} n^{3.25}$

Dit resultaat kunnen wij gebruiken om in polynomiale tijd te bepalen of een primitieve groep oplosbaar is. Dit doen we door het algoritme $GALOIS$ te laten lopen zolang de graad van de groep kleiner blijft dan in stelling 5.1, en als het algoritme geen groep gevonden heeft, dan weten we dat deze niet oplosbaar is. Als het algoritme wel een groep gevonden heeft, kunnen we in polynomiale tijd bepalen of deze oplosbaar is. Maar niet elke galoisgroep van een polynoom $f(x)$ werkt primitief op de wortels van $f(x)$. Wel kunnen we bepalen of $f(x)$ oplosbaar is in radicalen door te bepalen of alle tussenliggende uitbreidingen oplosbare uitbreidingen zijn. Volgens lemma 2.3 weten we dan dat $f(x)$ oplosbaar is in radicalen.

Dit is hoe het algoritme in zijn werk gaat. Eerst bepalen we een toren van lichaamsuitbreidingen tussen $\mathbb{Q}(\alpha)$ en $\mathbb{Q}$. Deze lichaamsuitbreidingen zijn zo geconstrueerd dat ze allemaal een primitieve galoisgroep hebben. Daarna kunnen we van elk van deze uitbreiding de galoisgroep bepalen, mits deze kleiner dan $24^{-1/3} n^{3,25}$ in orde is. Als dit niet zo is, is de groep ook niet oplosbaar volgens stelling 5.1. Algoritme 5.2 laat de pseudocode zien voor het algoritme.

Algoritme 5.2 OPLOSBAAR IN RADICALEN

1: **Input:** $f(x) \in \mathbb{Z}[x]$ monisch, irreducibel graad m.
2: Maak een toren van lichaamsuitbreidingen met $FIELDS(f(x))$
3: **for all** Uitbreidingen met minimaalpolynoom $g_i(x)$ en het basislichaam $\mathbb{Q}[x]/h_i(x)$ **do**
4: $G \leftarrow GALOIS'(g_i(x), \mathbb{Q}[x]/h_i(x))$
5: **if** $G = null$ **then**
6: return "Is niet oplosbaar in radicalen"
7: **else if** IS NOT $SOLVABLE(G)$ **then**
8: return "Is niet oplosbaar in radicalen"
9: **end if**
10: **end for**
11: return "Is oplosbaar in radicalen"

Het algoritme $GALOIS'$ is hetzelfde als in 5.1 met een kleine aanpassing. Als grootte van de groep (m in het algoritme) groter wordt dan $24^{-1/3}n^{3.25}$ stopt het algoritme. Want dan weten dat de galoisgroep niet oplosbaar is. De andere algoritmen worden in de volgende secties behandeld.

$FIELDS$ bepaalt de toren van (primitieve) lichaamsuitbreidingen en wordt behandelt in 5.4.

Dit algoritme gebruikt de subroutine $BLOCKS$, deze wordt eerst behandeld in 5.3.

Het algoritme $SOLVABLE$ bepaalt of een groep oplosbaar is, deze wordt behandelt in 5.5.

5.3 Minimaal imprimitief blok vinden

Met de stellingen uit 3.2 kunnen we een algoritme maken dat een minimaal imprimitief blok vindt. Hiervoor beschouwen we de factorisatie van $f(x)$ in $\mathbb{Q}(\alpha_1)$[x]. De corresponderende ondergroep van de galoisgroep is dan G_{α_1}. Als $f(x)$ opsplitst in meerdere lineaire factoren $(x - p_i(\alpha_1))$, dan worden de wortels $p_i(\alpha_1)$ ook gefixeerd door G_{α_1}. Uit stelling 3.2 volgt dan dat deze wortels samen een imprimitief blok vormen. We kunnen dan de groepstabel maken (net zoals in $GALOIS$) en daaruit een minimaal imprimitief blok vinden door het algoritme van Atkinson [3]. Als $f(x)$ niet opsplitst in meerdere lineaire factoren dan kunnen we stelling 3.3 gebruiken. We weten dan dat een minimaal imprimitief blok geschreven kan worden als de baan van α_1 onder $\langle G_{\alpha_1}, G_{\alpha_j} \rangle$ voor een andere wortel α_j in dit blok. Om te bepalen hoe deze baan eruit ziet beschouwen we de factorisatie van $f(x)$ in $\mathbb{Q}(\alpha_1)$ en in $\mathbb{Q}(\alpha_j)$:

$$f(x) = (x - \alpha_1)g_2(x)...g_r(x) \text{ in } \mathbb{Q}(\alpha_1)[x]$$

en

$$f(x) = (x - \alpha_j)h_2(x)...h_r(x) \text{ in } \mathbb{Q}(\alpha_j)[x]$$

waarbij $(x - \alpha_1) = g_1(x)$ en $(x - \alpha_j) = h_1(x)$.

Merk op dat de factorisatie gelijk aan elkaar zijn als je α_1 vervangt door α_j. We merken ook het volgende lemma op:

Lemma 5.2. *Als α_i een wortel is van $g_i(x)$ dan zijn $G_{\alpha_1}(\alpha_i)$ precies alle wortels van $g_i(x)$.*

De wortels van $f(x)$ worden binnen een willekeurige $h_i(x)$ gepermuteerd door G_{α_j} en binnen een willekeurige $g_i(x)$ gepermuteerd door G_{α_1}. Elk element van $\langle G_{\alpha_1}, G_{\alpha_j} \rangle$ is te schrijven als een product van elementen uit G_{α_1} en G_{α_j}. Zo kunnen we de baan bepalen van α_1 door te kijken waar deze wortel zit in $h_i(x)$ en dan te kijken in welke de wortels van $h_i(x)$ zitten in $\mathbb{Q}(\alpha_1)$etc. Dit doen we door middel van een graaf met punten V en kanten E:

$$V = \{g_i(x), i = 1, ..., r\} \cup \{h_i(x), i = 1, ..., r\}$$

$$E = \{< g_i(x), h_k(x) > \mid \text{ggd}(g_i(x), h_k(x)) \neq 1 \text{ over } \mathbb{Q}(\alpha_1, \alpha_j)\}$$

De graaf bestaat dus uit twee ontbindingen van $f(x)$ die met elkaar verbonden zijn als een factor uit de ene ontbinding een factor gemeen heeft met de andere ontbinding. Dan hebben ze namelijk een wortel gemeen. Deze graaf maken we $r-1$ keer. Elke keer is α_j een wortel van $g_i(x)$ voor $i = 2, ..., r$.

De factor $g_1(x) = (x - \alpha_1)$ is in elke graaf verbonden met een andere $h_k(x)$, dan permuteert G_{α_j} α_1 naar een andere wortel van $h_k(x)$, deze is weer te vinden in een $g_i(x)$, deze wordt dan weer gepermuteerd door G_{α_1} naar een andere wortel etc. Elk pad wat α_1 volgt is dus een aaneenschakeling van permutaties uit G_{α_1} en G_{α_j}. Dit betekent dat de wortels van alle factoren $g_i(x)$ waar $g_1(x)$ mee verbonden is, de baan vormen van α_1 door $\langle G_{\alpha_1}, G_{\alpha_j} \rangle$. We noemen het product van deze factoren $B_j(x)$.

Als we dit voor elke graaf doen, dan vormen de wortels van een dergelijk polynoom $B_J(x)$ met minimale graad een imprimitief blok volgens stelling 3.3.

Algoritme 5.3 Minimaal imprimitief blok ($BLOCKS$)

Input: $f(x) \in \mathbb{Q}[x]$
$\prod_i^r g_i(x) \leftarrow FACTOR(f(x))$ over $\mathbb{Q}[z]/f(z)$
if #lineaire factoren $g_i(x) > 1$ **then**
    Bereken de geïnduceerde actie van de galoisgroep op de lineaire factoren.
    Vind het minimale blok met Atkinson [3].
    Return $\prod$ (lineaire factoren in het minimale blok.)
else
    for all $1 < j \leq r$ **do**
        Maak een graaf:
        $V = \{g_i(x), i = 1, ..., r\} \cup \{h_i(x), i = 1, ..., r\}$
        $E = \{< g_i(x), h_k(x) > \mid \text{ggd}(g_i(x), h_k(x) \neq 1 \text{ over } \mathbb{Q}(\alpha_1, \alpha_j)\}$
        $B_j(x) \leftarrow \prod\{g_t(x) | g_t(x) \text{ is verbonden met } g_1(x)\}$
    end for
    Return $B_j(x)$ met minimale graad
end if

Om de kanten van de graaf te maken moeten we kijken naar factorisatie van $f(x)$ in $\mathbb{Q}(\alpha_1, \alpha_j)$. We kunnen hiervoor het algoritme van Landau [8] gebruiken. Zo vinden we een primitief element voor dit lichaam en kunnen we de factoren $g_i(x)$ en $h_k(x)$ omschrijven naar dit lichaam, en dan kunnen we de grootste gemeenschappelijke deler bepalen van twee factoren $g_i(x)$ en $h_k(x)$ over $\mathbb{Q}(\alpha_1, \alpha_j)$.

5.4 Toren van lichaamsuitbreidingen maken

Om een toren van (primitieve) lichaamsuitbreidingen te maken merken we het volgende op over imprimitieve blokken van $f(x)$:

Stelling 5.3. *Laat $f(x)$ een polynoom zijn met wortels $\{\alpha_1, ..., \alpha_m\}$ en laat B een minimaal imprimitief blok zijn van wortels $\{\alpha_1, ..., \alpha_k\}$. Neem dan:*

$$g(x) = \prod_{i=1}^{k} (x - \alpha_i) = x^k + \beta_{k-1}x^{k-1} + ... + \beta_0.$$

Dan is $g(x)$ de minimaalpolynoom voor α_1 over $F = \mathbb{Q}(\beta_0, \beta_1, ..., \beta_{k-1})$.

Bewijs:

- F is een deellichaam van $\mathbb{Q}(\alpha_1)$ volgens de hoofdstelling van de Galoistheorie (stelling 2.1) met $G_{\alpha_1} < G_B$ (lemma 3.1) .
- α_1 is een wortel van $g(x)$.

- $[\mathbb{Q}(\alpha) : F] = [\mathbb{Q}(\alpha_1, ...\alpha_k) : F]/[\mathbb{Q}(\alpha_1, ...\alpha_k) : \mathbb{Q}(\alpha_1)] = |G_B|/|G_\alpha| = k.\square$

Dit kunnen we gebruiken om het eerste deellichaam van $\mathbb{Q}(\alpha)$ te bepalen. We nemen een minimaal imprimitief blok van $f(x)$ zoals beschreven in de vorige sectie, dit geeft ons $g_1(x)$. De coëfficiënten van deze polynoom vormen dan het nieuwe lichaam $F = \mathbb{Q}(\beta_0, \beta_1, ..., \beta_{k-1})$. Deze coëfficiënten zijn de elementaire symmetrische functies van het blok $\{\alpha_1, ..., \alpha_k\}$. Voor dit lichaam kunnen we een primitief element ρ maken. En daarna kunnen we voor ρ een minimaalpolynoom $h_1(x)$ maken. Zo hebben we het lichaam $\mathbb{Q}[x]/(h_1(x)) \cong \mathbb{Q}(\rho)$ gecreëerd. We schrijven dan de coëfficiënten van $g_1(x)$ om in termen van het primitieve element ρ. Omdat we $g_1(x)$ gemaakt hebben van een minimaal imprimitief blok, weten we dat de galoisgroep primitief werkt op de wortels van $g_1(x)$. Zo hebben we de eerste primitieve uitbreiding gemaakt.

Nu we $\mathbb{Q}[x]/(h_1(x))$ hebben, kunnen we van $h_1(x)$ weer een minimaal imprimitief blok vinden. Zo kunnen we op dezelfde manier een deellichaam vinden van $\mathbb{Q}[x]/(h_1(x))$. Dit blijven we doen totdat er geen non-triviaal blok meer is van $h_r(x)$. Dan werkt de galoisgroep van $h_r(x)$ over $\mathbb{Q}$ primitief op de wortels van $h_r(x)$. Zo hebben we twee rijen van polynomen $g_i(x)$ en $h_i(x)$ gemaakt waarvoor geldt:

- $h_i(x) \in \mathbb{Q}[x]$
- $g_i(y) \in \mathbb{Q}[x, y]/h_i(x)$
- De galoisgroep van $g_i(y)$ over $\mathbb{Q}[x]/h_i(x)$ werkt primitief op de wortels van $g_i(y)$.
- De galoisgroep van $h_r(x)$ over $\mathbb{Q}$ werkt primitief op de wortels van $h_r(x)$.

Algoritme 5.4 Toren van lichaamsuitbreidingen ($FIELDS$)

Input: $f(x) \in \mathbb{Q}[x]$
$B^z(x) \leftarrow x^k + \beta_{k-1}(z)x^{k-1} + ... + \beta_0(z) \leftarrow BLOCKS(f(x))$
$i = 1$
while $B^z(x) \notin \mathbb{Q}[x]$ **do**
    $\rho(z) \leftarrow \beta_0(z)$
    for $i = 1..., k-1$ **do**
        $\rho(z) \leftarrow PrimitiefElement(\rho(z), \beta_i(z))$
    end for
    $h_i(x) \leftarrow MinimaalPolynoom(\rho(z))$
    for $j = 0, ..., k-1$ **do**
        Vind $p_j(x)$ zodat $p_j(\rho(z)) = \beta(z)$
    end for
    $g_i(y) \leftarrow y^k + p_{k-1}(z)y^{k-1} + ... + p_0(z)$
    $i \leftarrow i + 1$
end while
return $\{g_i(x), h_i(x) | i = 1, ..., r\}$

Zo hebben we een aantal lichamen $\mathbb{Q}[x]/(h_i(x))$ en een aantal minimaalpolynomen $g_i(y)$ gemaakt, zodat deze het bovenliggende lichaam definiëren. Hierbij is de laatste minimaalpolynoom een polynoom in $\mathbb{Q}$.

5.5 Oplosbaarheid bepalen

Als we een groepstabel van G hebben gekregen uit het algoritme $GALOIS'$, dan is deze polynomiaal in grootte. We moeten dan nog bepalen of deze oplosbaar is. Dit kunnen we op verschillende manieren doen. Ter demonstratie zal ik er hier een uitleggen. We gebruiken lemma 2.4. We kunnen de commutatorreeks maken door eerst de commutators te maken van alle elementen in G. Deze laten we dan de rest van de groep voortbrengen en zo hebben we de 1^e ondergroep gemaakt. We gaan door totdat de orde van de groep gelijk blijft. Als dit aantal 1 is, dan is de groep oplosbaar en anders niet.

Algoritme 5.5 Oplosbare groep ($SOLVABLE$)

Input: Vermenigvuldigingstabel van groep G.
$J \leftarrow \{ghg^{-1}h^{-1} | \forall g, h \in G\}$
$H = \{e\}$
while $|H| < |J|$ **do** ▷ H is de groep voortgebracht door commutators.
    $H \leftarrow J$
    $J \leftarrow J \cup \{gh | \forall g, h \in J\}$
end while
if $|H| < |G|$ **then**
    $G \leftarrow H$
    Ga naar 2:
end if
if $|H| = 1$ **then**
    return "G is oplosbaar"
else
    return "G is niet oplosbaar"
end if

6 Looptijd analyse

De looptijd analyse breekt op in een aantal delen. Allereerst bepalen we namelijk een toren van lichaamsuitbreidingen en daarna bepalen we voor elke uitbreiding een de galoisgroep, mits deze kleiner is dan $24^{-1/3}n^{3,25}$. Van deze galoisgroep bepalen we of deze oplosbaar is.

De looptijd van dit algoritme is dus gelijk aan de looptijd van het maken van de toren plus het aantal lichaamsuitbreidingen vermenigvuldigt met de looptijd voor het vinden van de galoisgroep en zijn oplosbaarheid bepalen. Dus de looptijd $= O(FIELDS + \#Uitbreidingen * (GALOIS' + SOLVABLE))$.

De looptijd voor $SOLVABLE$ is als volgt uit te rekenen: Stel de input is een vermenigvuldigingstabel van G met n elementen. Dan maken we een commutator in $O(1)$ tijd voor alle paren van elementen. Dit kost dus $O(n^2)$. Vervolgens laten we deze elementen de rest van groep genereren. We maken het product van alle paren in deze verzameling en blijven dit itereren tot de verzameling niet groter wordt. Dit kan in ieder geval niet vaker dan n keer (de limiet kan nog veel beter). Nu hebben we de 1^e ondergroep gecreëerd in maximaal $O(n^3)$ tijd. Omdat we een ondergroep van G hebben gegenereerd,heeft deze een orde van ten hoogste n. Als de orde n is, stopt het algoritme, en anders is het een echte ondergroep en is de orde $\leq n^2$ Van deze groep maken we weer een ondergroep etc. De looptijd is dus van de orde:

$$O(\sum_{i=0}^{log_2 n}(\frac{n^3}{2^i})) = O(n^3 \sum_{i=0}^{log_2 n}(\frac{1}{2^i})) = O(n^3)$$

De looptijd van $GALOIS$ breekt op in twee delen: In het eerste deel blijven we wortels toevoegen en $f(x)$ factoriseren. Dit kan hoogstens $deg(f)$ keer. Ook berekenen we elke stap een primitief element en een minimaalpolynoom voor dit element. Tijdens het factoriseren van $f(x)$ over een lichaam krijgen we in constante tijd een primitief element voor het volgende lichaam [8], dus dat kunnen we buiten beschouwing laten. De graad van het minimaalpolynoom is op het einde van algoritme de orde van de galoisgroep. Het vinden van een minimaalpolynoom is een lineair onafhankelijkheidsprobleem. De looptijd hiervan is $O(m^5)$, waarbij m de graad is van het minimaalpolynoom [4]. De looptijd voor het eerste gedeelte is dus maximaal $O(deg(f) * (FACTOR(f) + |G|^5))$. Omdat we algoritme stop zetten wanneer de galoisgroep groter dan $24^{-1/3}deg(f)^{3,25}$, is de looptijd maximaal $O(deg(f) * (FACTOR(f) + deg(f)^{16}))$.

Het tweede gedeelte combineert alle factoren van $f(x)$ en het minimaalpolynoom voor het splijtli-

chaam. Het aantal factoren van de minimaalpolynoom is gelijk aan de orde van de galoisgroep. Het berekenen van de compositie kan in $O(1)$ tijd. De looptijd voor dit gedeelte is dus $O(deg(f) * |G|) = O(deg(f)^{4,25})$.

Het algoritme $FIELDS$ maakt een toren van lichaamsuitbreidingen tussen $\mathbb{Q}$ en $\mathbb{Q}(\alpha)$. De graad van de volledige uitbreiding $\mathbb{Q}(\alpha)/\mathbb{Q} = deg(f)$. We weten dat $[K : M] = [K : L] * [L : M]$ voor $M \subset L \subset K$. Er kunnen dus hoogstens $log_2(deg(f))$ tussenliggende uitbreidingen zijn.

De looptijd van $FIELDS$ breekt op in een aantal verschillende stappen. Allereerst bepalen we een minimaal imprimitief blok, dan bepalen we een primitief element, en vervolgens een minimaalpolynoom voor dit element. Dit doen we totdat we $\mathbb{Q}$ hebben bereikt. We weten dat er maximaal $log(deg(f))$ iteraties zijn.

De looptijd voor $FIELDS$ is dus maximaal $O((BLOCKS+PrimitiefElement+MinimaalPolynoom)* log(deg(f)))$

De looptijd van het bepalen van een primitief element voor $\mathbb{Q}(\beta_1, ..., \beta_k)$, kost maximaal $k-1$ keer de tijd om een primitief element te vinden voor twee elementen.

We weten dat er een maximum is voor het aantal $c \in \mathbb{Z}$ waarvoor $\mathbb{Q}(\alpha + c\beta)$ niet gelijk is aan $\mathbb{Q}(\alpha, \beta)$. Dit maximum is gelijk aan $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$ [13]. De graad van $\mathbb{Q}(\beta_1, ..., \beta_k)/\mathbb{Q}$ is gelijk aan $[\mathbb{Q}(\alpha) : \mathbb{Q}]/[\mathbb{Q}(\alpha) : \mathbb{Q}(\beta_1, ..., \beta_k)] = deg(f)/k$ (zie stelling 5.3). Het maximum aantal $c \in \mathbb{Z}$ is dus gelijk aan $deg(f)/k$.

Het controleren of een element een lichaam genereert, is een simpel lineair onafhankelijkheidsprobleem. Dit is gelimiteerd door $O(m^5)$ [4]. Hierbij is m de graad van de uitbreiding (dus $deg(f)/k$) Het vinden van een primitief element kost dus maximaal $O(k * (deg(f)/k)^6)$. Omdat k altijd kleiner is dan $deg(f)$, kan de looptijd dus worden gelimiteerd door $O(deg(f)^6)$.

Het vinden van een minimaalpolynoom is ook een lineair onafhankelijkheidsprobleem met dezelfde dimensie als de graad van de uitbreiding en wordt dus gedomineerd door de looptijd van het vinden van een primitief element.

Het vinden van een minimaal imprimitief blok is te onderscheiden in twee gevallen. Of $f(x)$ splits in meerdere lineaire factoren in $\mathbb{Q}[z]/f(z)$, of doet dat niet. In het eerste geval bepalen we een minimaal imprimitief blok door middel van de geïnduceerde actie en Atkinsons' algoritme [3]. De looptijd is dus maximaal $O(FACTOR(f(x)) + InducedAction + Atkinson)$.

Het vinden van de geïnduceerde actie doe je door twee lineaire factoren te combineren en te kijken naar welke andere factor dit wordt afgebeeld. Dit kost dus $O(r^2)$, waarbij r het aantal lineaire factoren is. Dit is maximaal $deg(f)$.

Het algoritme van Atkinson is polynomiaal in de orde van de groep [3] en dus polynomiaal in de graad van $f(x)$.

In het tweede geval factoriseren we $f(x)$ over twee wortels. Daarna bepalen we de grootste gemeenschappelijke deler van alle paren uit de (eerste) factorisatie. En daarna lopen we de graaf door om een blok te vinden. We maken evenveel grafen als niet-lineaire factoren van $f(x)$ in $\mathbb{Q}[z]/f(z)$. Het aantal niet-lineaire factoren is kleiner dan $deg(f)/2$. Dit aantal noemen we r. We factoriseren $f(x)$ dus r keer over een lichaam van 2 wortels. Elke keer bepalen we dan r^2 grootste gemeenschappelijke delers van de factoren van $f(x)$. In totaal bepalen we dus r^3 keer de grootste gemeenschappelijke deler van twee polynomen die graad kleiner dan die van $f(x)$ hebben. De looptijd om de graaf door te lopen is verwaarloosbaar in vergelijking met de vorige stappen. Het bepalen van een grootste gemeenschappelijke deler van twee polynomen is lineair in de graad van grootste polynoom. De looptijd is maximaal $O(r * FACTOR(f) + r^3 * deg(f)))$.

Volgens Landau [8] is de looptijd van factoriseren van $f(x)$ over een eindige lichaamsuitbreiding van $\mathbb{Q}$ polynomiaal in de graad van $f(x)$.

De looptijd van $BLOCKS$ is dus in beide gevallen polynomiaal in de graad van $f(x)$. Als we dan alles combineren zien we dat de looptijd van dit algoritme polynomiaal is in de graad van $f(x)$.

7 Afsluiting

We hebben nu een manier gevonden om van een willekeurige polynoom te bepalen of deze oplosbaar is in radicalen. Dit doen we zelfs in polynomiale tijd in de graad van de polynoom. We hebben hiermee niet de galoisgroep gevonden van de polynoom en ook niet de oplossingen. Het "snel" vinden van de galoisgroep blijft nog steeds een onopgelost probleem.

Het vinden van de oplossingen van de polynoom kan wel gedaan worden met (een aanpassing) van dit algoritme. Landau [9] beschrijft hier hetzelfde algoritme, maar maakt een kleine aanpassing tijdens het maken van een nieuw deellichaam in $FIELDS$. Waar wij alleen in de eerste stap een lichaam creëren in de symmetrische functies van een imprimitief blok van wortels van $f(x)$, doet zij dit in elke stap. Zo kan er later makkelijker worden teruggerekend wat de wortels van $f(x)$ zijn. Ook beschrijft Landau [9] hoe groot de coëfficiënten worden van alle polynomen tijdens het algoritme, en bewijst dat deze binnen polynomiale limieten blijven.

Referenties

[1] Asger Aaboe. *Episodes from the early history of mathematics.* New mathematical library. Mathematical Association of America, 1964.

[2] Niels H. Abel and Ludwig Sylow. *Oeuvres Complètes de Niels Henrik Abel: Nouvelle Édition. Volume 1.* Number v. 1 in Cambridge Library Collection - Mathematics. Cambridge University Press, 1881.

[3] Michael D. Atkinson. An algorithm for finding the blocks of a permutation group. *Math. Comput.*, 29:911–913, 1975.

[4] Jack Edmonds. Systems of distinct representatives and linear algebra. *J. Res. Nat. Bur. Standards Sect. B*, 71B:241–245, 1967.

[5] Gertrude Ehrlich. *Fundamental Concepts of Abstract Algebra.* Dover Books on Mathematics Series. Dover Publications, 2011.

[6] H. Kurzweil and B. Stellmacher. *The Theory of Finite Groups: An Introduction.* Universitext. Springer New York, 2003.

[7] Susan Landau. *On computing Galois groups and its application to solvability by radicals.* ProQuest LLC, Ann Arbor, MI, 1983. Thesis (Ph.D.)–Massachusetts Institute of Technology.

[8] Susan Landau. Factoring polynomials over algebraic number fields. *SIAM J. Comput.*, 14(1):184–195, 1985.

[9] Susan Landau and Gary Lee Miller. Solvability by radicals is in polynomial time. *J. Comput. System Sci.*, 30(2):179–208, 1985.

[10] Arjen K. Lenstra, Hendrik W. Lenstra, Jr., and László Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261(4):515–534, 1982.

[11] Péter P. Pálfy. A polynomial bound for the orders of primitive solvable groups. *J. Algebra*, 77(1):127–137, 1982.

[12] Mikhail Postnikov and Ann Swinfen. *Foundations of Galois Theory.* Dover books on mathematics. Dover Publications, 2004.

[13] Kazuhiro Yokoyama, Masayuki Noro, and Taku Takeshima. Computing primitive elements of extension fields. *J. Symbolic Comput.*, 8(6):553–580, 1989.