The Monogeneity of Kummer Extensions and Radical Extensions

Hanson Smith

University of Colorado, Boulder

Table of contents

Motivation and Background

A Quadratic Field

Consider $\mathbb{Q}\left(\sqrt{17}\right)$.

A Quadratic Field

Consider $\mathbb{Q}\left(\sqrt{17}\right)$.

The discriminant is 17, so 17 is the only ramified prime.

A Quadratic Field

Consider $\mathbb{Q}\left(\sqrt{17}\right)$.

The discriminant is 17, so 17 is the only ramified prime.

A prime p other than 17 splits if and only if $17 \equiv a^2 \bmod p$.

A Quadratic Field

Consider $\mathbb{Q}\left(\sqrt{17}\right)$.

The discriminant is 17, so 17 is the only ramified prime.

A prime p other than 17 splits if and only if $17 \equiv a^2 \bmod p$.

The ring of integers is $\mathbb{Z}\left[\frac{1+\sqrt{17}}{2}\right]$.

A Cyclotomic Field

Consider $\mathbb{Q}(\zeta_5)$.

A Cyclotomic Field

Consider $\mathbb{Q}(\zeta_5)$.

The discriminant is 5^3, so 5 is the only ramified prime.

A Cyclotomic Field

Consider $\mathbb{Q}(\zeta_5)$.

The discriminant is 5^3, so 5 is the only ramified prime.

The inertia degree of a prime p other than 5 is the least positive integer f such that $p^f \equiv 1 \bmod 5$.

A Cyclotomic Field

Consider $\mathbb{Q}(\zeta_5)$.

The discriminant is 5^3, so 5 is the only ramified prime.

The inertia degree of a prime p other than 5 is the least positive integer f such that $p^f \equiv 1 \bmod 5$.

The ring of integers is $\mathbb{Z}[\zeta_5]$.

A Kummer Extension

Consider $\mathbb{Q}\left(\zeta_5, \sqrt[5]{23}\right)$.

A Kummer Extension

Consider $\mathbb{Q}\left(\zeta_5, \sqrt[5]{23}\right)$.

The discriminant is $5^{23} \cdot 23^{16}$, so 5 and 23 are the only ramified primes.

A Kummer Extension

Consider $\mathbb{Q}\left(\zeta_5, \sqrt[5]{23}\right)$.

The discriminant is $5^{23} \cdot 23^{16}$, so 5 and 23 are the only ramified primes.

The inertia degree of a prime $\mathfrak{p}$ of $\mathbb{Z}[\zeta_5]$ other than the primes above 5 and 23 is the least positive integer f such that $23^f \equiv x^5 \bmod \mathfrak{p}$ is solvable.

A Kummer Extension

Consider $\mathbb{Q}\left(\zeta_5, \sqrt[5]{23}\right)$.

The discriminant is $5^{23} \cdot 23^{16}$, so 5 and 23 are the only ramified primes.

The inertia degree of a prime $\mathfrak{p}$ of $\mathbb{Z}[\zeta_5]$ other than the primes above 5 and 23 is the least positive integer f such that $23^f \equiv x^5 \bmod \mathfrak{p}$ is solvable.

The ring of integers...

$$\frac{279131255861}{371131200000} b_1^{19} + \frac{139394830991}{371131200000} b_1^{18} + \frac{60448487777}{123710400000} b_1^{17} + \frac{280219029161}{371131200000} b_1^{16} +$$
$$\frac{94145035483}{185565600000} b_1^{15} + \frac{44239217807}{371131200000} b_1^{14} + \frac{4438720949}{46391400000} b_1^{13} + \frac{70969469297}{371131200000} b_1^{12} +$$
$$\frac{2509087807}{371131200000} b_1^{11} + \frac{56229143}{2577300000} b_1^{10} + \frac{113716751}{123710400000} b_1^{9} + \frac{22518667}{92782800000} b_1^{8} +$$
$$\frac{3810863}{371131200000} b_1^{7} + \frac{51769603}{371131200000} b_1^{6} + \frac{44967809}{185565600000} b_1^{5} + \frac{1736227}{185565600000} b_1^{4} +$$
$$\frac{3749}{371131200000} b_1^{3} + \frac{1}{966487500} b_1^{2} + \frac{1}{161081250} b_1 + \frac{1}{26846875}, \frac{2722605997}{24742080000} b_1^{19} +$$
$$\frac{7264409407}{24742080000} b_1^{18} + \frac{2635174187}{2749120000} b_1^{17} + \frac{6255406393}{24742080000} b_1^{16} + \frac{168842561}{224928000} b_1^{15} +$$
$$\frac{2269014439}{24742080000} b_1^{14} + \frac{52199291}{386595000} b_1^{13} + \frac{2534812681}{24742080000} b_1^{12} + \frac{910778831}{24742080000} b_1^{11} + \frac{216703}{6248000} b_1^{10} +$$
$$\frac{3915709}{2749120000} b_1^{9} + \frac{423989}{6185520000} b_1^{8} + \frac{1248439}{24742080000} b_1^{7} + \frac{2807459}{24742080000} b_1^{6} + \frac{38131}{224928000} b_1^{5} +$$
$$\frac{729779}{12371040000} b_1^{4} + \frac{13}{24742080000} b_1^{3} + \frac{1}{343640000} b_1^{2} + \frac{1}{128865000} b_1, \frac{119802319}{168696000} b_1^{19} +$$
$$\frac{6689293}{42174000} b_1^{18} + \frac{5183347}{12780000} b_1^{17} + \frac{28338223}{42174000} b_1^{16} + \frac{168250549}{168696000} b_1^{15} + \frac{18297679}{168696000} b_1^{14} +$$
$$\frac{29305517}{168696000} b_1^{13} + \frac{126539399}{843480000} b_1^{12} + \frac{29777}{1917000} b_1^{11} + \frac{28789}{5112000} b_1^{10} + \frac{4073}{11246400} b_1^{9} +$$
$$\frac{9607}{33739200} b_1^{8} + \frac{13711}{76680000} b_1^{7} + \frac{3991}{84348000} b_1^{6} + \frac{57239}{168696000} b_1^{5} + \frac{929}{21087000} b_1^{4} +$$
$$\frac{1}{168696000} b_1^{3} + \frac{1}{281160000} b_1^{2}, \frac{86803537}{95040000} b_1^{19} + \frac{50731939}{95040000} b_1^{18} + \frac{1954979}{2112000} b_1^{17} +$$
$$\frac{14813297}{19008000} b_1^{16} + \frac{5502451}{9504000} b_1^{15} + \frac{18005539}{95040000} b_1^{14} + \frac{919681}{11880000} b_1^{13} + \frac{298123}{1728000} b_1^{12} +$$
$$\frac{26501}{1728000} b_1^{11} + \frac{607}{36000} b_1^{10} + \frac{52387}{31680000} b_1^{9} + \frac{5903}{23760000} b_1^{8} + \frac{6311}{19008000} b_1^{7} + \frac{667}{19008000} b_1^{6} +$$
$$\frac{3401}{9504000} b_1^{5} + \frac{1319}{47520000} b_1^{4} + \frac{1}{95040000} b_1^{3}, \frac{4842}{6875} b_1^{19} + \frac{2683}{13750} b_1^{14} + \frac{7}{13750} b_1^{9} +$$
$$\frac{1}{13750} b_1^{4}, \frac{702}{1375} b_1^{19} + \frac{19}{25} b_1^{18} + \frac{7}{25} b_1^{17} + \frac{1891}{2750} b_1^{15} + \frac{11}{125} b_1^{14} + \frac{1}{25} b_1^{13} + \frac{3}{25} b_1^{12} +$$

A Kummer Extension

Can we write the ring of integers of $\mathbb{Q}\left(\zeta_5, \sqrt[5]{23}\right)$, denoted $\mathcal{O}_{\mathbb{Q}\left(\zeta_5, \sqrt[5]{23}\right)}$, as $\mathbb{Z}[\alpha]$ for some α?

A Kummer Extension

Can we write the ring of integers of $\mathbb{Q}\left(\zeta_5, \sqrt[5]{23}\right)$, denoted $\mathcal{O}_{\mathbb{Q}\left(\zeta_5, \sqrt[5]{23}\right)}$, as $\mathbb{Z}[\alpha]$ for some α?

Can we write $\mathcal{O}_{\mathbb{Q}\left(\zeta_5, \sqrt[5]{23}\right)}$ as $\mathbb{Z}\left[\zeta_5\right]\left[\alpha\right]$?

Monogeneity

Let M be an extension of a number field L. We say M is **monogenic relative to** L if $\mathcal{O}_L[\alpha] = \mathcal{O}_M$.

Monogeneity

Let M be an extension of a number field L. We say M is **monogenic relative to** L if $\mathcal{O}_L[\alpha] = \mathcal{O}_M$. In this case we say that $\mathcal{O}_M$ admits a **power $\mathcal{O}_L$-integral basis**.

Monogeneity

Let M be an extension of a number field L. We say M is **monogenic relative to** L if $\mathcal{O}_L[\alpha] = \mathcal{O}_M$. In this case we say that $\mathcal{O}_M$ admits a **power** $\mathcal{O}_L$**-integral basis**. If $L = \mathbb{Q}$, we simply say M is monogenic and $\mathcal{O}_M$ admits a power integral basis.

Monogeneity

Let M be an extension of a number field L. We say M is **monogenic relative to** L if $\mathcal{O}_L[\alpha] = \mathcal{O}_M$. In this case we say that $\mathcal{O}_M$ admits a **power** $\mathcal{O}_L$**-integral basis**. If $L = \mathbb{Q}$, we simply say M is monogenic and $\mathcal{O}_M$ admits a power integral basis.

As we've seen, all quadratic fields and cyclotomic fields are monogenic.

Monogeneity

Let M be an extension of a number field L. We say M is **monogenic relative to** L if $\mathcal{O}_L[\alpha] = \mathcal{O}_M$. In this case we say that $\mathcal{O}_M$ admits a **power** $\mathcal{O}_L$**-integral basis**. If $L = \mathbb{Q}$, we simply say M is monogenic and $\mathcal{O}_M$ admits a power integral basis.

As we've seen, all quadratic fields and cyclotomic fields are monogenic.

Dedekind was the first person to give an example of a non-monogenic field: $\mathbb{Q}(\alpha)$ where α is a root of $x^3 - x^2 - 2x - 8$.

Monogeneity

Let M be an extension of a number field L. We say M is **monogenic relative to** L if $\mathcal{O}_L[\alpha] = \mathcal{O}_M$. In this case we say that $\mathcal{O}_M$ admits a **power $\mathcal{O}_L$-integral basis**. If $L = \mathbb{Q}$, we simply say M is monogenic and $\mathcal{O}_M$ admits a power integral basis.

As we've seen, all quadratic fields and cyclotomic fields are monogenic.

Dedekind was the first person to give an example of a non-monogenic field: $\mathbb{Q}(\alpha)$ where α is a root of $x^3 - x^2 - 2x - 8$. We'll return to Dedekind's ideas.

Monogeneity

Let M be an extension of a number field L. We say M is **monogenic relative to** L if $\mathcal{O}_L[\alpha] = \mathcal{O}_M$. In this case we say that $\mathcal{O}_M$ admits a **power $\mathcal{O}_L$-integral basis**. If $L = \mathbb{Q}$, we simply say M is monogenic and $\mathcal{O}_M$ admits a power integral basis.

As we've seen, all quadratic fields and cyclotomic fields are monogenic.

Dedekind was the first person to give an example of a non-monogenic field: $\mathbb{Q}(\alpha)$ where α is a root of $x^3 - x^2 - 2x - 8$. We'll return to Dedekind's ideas.

When are Kummer extensions (and more generally radical, $\sqrt[n]{\bullet}$, extensions) monogenic?

Results

Main Result for Kummer Extensions

Theorem (Smith)

Let p be a rational prime. Note $(1 - \zeta_p)$ is the unique prime of $\mathbb{Z}[\zeta_p]$ above p.

Main Result for Kummer Extensions

Theorem (Smith)

Let p be a rational prime. Note $(1-\zeta_p)$ is the unique prime of $\mathbb{Z}[\zeta_p]$ above p. Let $\alpha \in \mathbb{Z}[\zeta_p]$, and suppose that $x^p - \alpha$ is irreducible in $\mathbb{Z}[\zeta_p][x]$.

Main Result for Kummer Extensions

Theorem (Smith)

Let p be a rational prime. Note $(1 - \zeta_p)$ is the unique prime of $\mathbb{Z}[\zeta_p]$ above p. Let $\alpha \in \mathbb{Z}[\zeta_p]$, and suppose that $x^p - \alpha$ is irreducible in $\mathbb{Z}[\zeta_p][x]$. Consider $\mathbb{Q}\left(\zeta_p, \sqrt[p]{\alpha}\right)$.

Main Result for Kummer Extensions

Theorem (Smith)

Let p be a rational prime. Note $(1-\zeta_p)$ is the unique prime of $\mathbb{Z}[\zeta_p]$ above p. Let $\alpha \in \mathbb{Z}[\zeta_p]$, and suppose that $x^p - \alpha$ is irreducible in $\mathbb{Z}[\zeta_p][x]$. Consider $\mathbb{Q}\left(\zeta_p, \sqrt[p]{\alpha}\right)$. The ring of integers $\mathcal{O}_{\mathbb{Q}\left(\zeta_p, \sqrt[p]{\alpha}\right)}$ is $\mathbb{Z}[\zeta_p]\left[\sqrt[p]{\alpha}\right]$ if and only if α is square-free as an ideal of $\mathbb{Z}[\zeta_p]$ and the congruence

$$\alpha^p \equiv \alpha \bmod (1-\zeta_p)^2 \tag{1}$$

is not *satisfied.*

Main Result for Kummer Extensions

Marie-Nicole Gras[1] has shown that the only monogenic cyclic extensions of $\mathbb{Q}$ of prime degree ≥ 5 are maximal real subfields of cyclotomic fields.

[1] M.-N. Gras. Non monogénéité de l'anneau des entiers des extensions cycliques de $\mathbb{Q}$ de degré premier $l \geq 5$. J. Number Theory, 23(3):347–353, 1986.

Main Result for Kummer Extensions

Marie-Nicole Gras[1] has shown that the only monogenic cyclic extensions of $\mathbb{Q}$ of prime degree ≥ 5 are maximal real subfields of cyclotomic fields.

Over $\mathbb{Q}(\zeta_p)$, however, we can construct infinitely many cyclic extensions of degree p that are monogenic.

[1] M.-N. Gras. Non monogénéité de l'anneau des entiers des extensions cycliques de $\mathbb{Q}$ de degré premier $l \geq 5$. J. Number Theory, 23(3):347–353, 1986.

Main Result for Kummer Extensions

Marie-Nicole Gras[1] has shown that the only monogenic cyclic extensions of $\mathbb{Q}$ of prime degree ≥ 5 are maximal real subfields of cyclotomic fields.

Over $\mathbb{Q}(\zeta_p)$, however, we can construct infinitely many cyclic extensions of degree p that are monogenic.

Specifically, $\mathbb{Q}\left(\zeta_p, \sqrt[p]{\beta(1-\zeta_p)}\right)$ is monogenic over $\mathbb{Q}(\zeta_p)$ with generator $\sqrt[p]{\beta(1-\zeta_p)}$ for any square-free β that is prime to $1-\zeta_p$.

[1] M.-N. Gras. Non monogénéité de l'anneau des entiers des extensions cycliques de $\mathbb{Q}$ de degré premier $l \geq 5$. J. Number Theory, 23(3):347–353, 1986.

The Main Result

Let L be a number field and $\alpha \in \mathcal{O}_L$ be such that $x^n - \alpha$ is irreducible over L.

The Main Result

Let L be a number field and $\alpha \in \mathcal{O}_L$ be such that $x^n - \alpha$ is irreducible over L. For a prime $\mathfrak{p}$ of $\mathcal{O}_L$, we write p for the residue characteristic and f for the residue class degree.

The Main Result

Let L be a number field and $\alpha \in \mathcal{O}_L$ be such that $x^n - \alpha$ is irreducible over L. For a prime $\mathfrak{p}$ of $\mathcal{O}_L$, we write p for the residue characteristic and f for the residue class degree. If $\mathfrak{p}$ divides n, we factor $n = p^e m$ with $\gcd(m, p) = 1$. Define ε to be congruent to e modulo f with $1 \leq \varepsilon \leq f$.

The Main Result

Let L be a number field and $\alpha \in \mathcal{O}_L$ be such that $x^n - \alpha$ is irreducible over L. For a prime $\mathfrak{p}$ of $\mathcal{O}_L$, we write p for the residue characteristic and f for the residue class degree. If $\mathfrak{p}$ divides n, we factor $n = p^e m$ with $\gcd(m, p) = 1$. Define ε to be congruent to e modulo f with $1 \leq \varepsilon \leq f$. The Wieferich congruence becomes

$$\alpha^{p^{f-\varepsilon+e}} \equiv \alpha \bmod \mathfrak{p}^2. \tag{2}$$

The Main Result

Let L be a number field and $\alpha \in \mathcal{O}_L$ be such that $x^n - \alpha$ is irreducible over L. For a prime $\mathfrak{p}$ of $\mathcal{O}_L$, we write p for the residue characteristic and f for the residue class degree. If $\mathfrak{p}$ divides n, we factor $n = p^e m$ with $\gcd(m, p) = 1$. Define ε to be congruent to e modulo f with $1 \leq \varepsilon \leq f$. The Wieferich congruence becomes

$$\alpha^{p^{f-\varepsilon+e}} \equiv \alpha \bmod \mathfrak{p}^2. \tag{2}$$

In the case where $e \leq f$, this is

$$\alpha^{p^f} \equiv \alpha \bmod \mathfrak{p}^2.$$

The Main Result

Let L be a number field and $\alpha \in \mathcal{O}_L$ be such that $x^n - \alpha$ is irreducible over L. For a prime $\mathfrak{p}$ of $\mathcal{O}_L$, we write p for the residue characteristic and f for the residue class degree. If $\mathfrak{p}$ divides n, we factor $n = p^e m$ with $\gcd(m, p) = 1$. Define ε to be congruent to e modulo f with $1 \leq \varepsilon \leq f$. The Wieferich congruence becomes

$$\alpha^{p^{f-\varepsilon+e}} \equiv \alpha \bmod \mathfrak{p}^2. \tag{2}$$

In the case where $e \leq f$, this is

$$\alpha^{p^f} \equiv \alpha \bmod \mathfrak{p}^2.$$

Theorem (Smith)

The ring of integers of $L(\sqrt[n]{\alpha})$ is $\mathcal{O}_L[\sqrt[n]{\alpha}]$ if and only if α is square-free as an ideal of $\mathcal{O}_L$ and every prime $\mathfrak{p}$ dividing n **does not** *satisfy Congruence* (2)*.*

Non-monogeneity of Kummer Extensions

Theorem (Smith)

Denote $\mathbb{Q}(\zeta_n, \sqrt[n]{\alpha})$ *by* K*, and suppose there exists a rational prime* ℓ *such that* $\ell \equiv 1 \bmod n$ *and* $\ell < n \cdot \phi(n)$*.*

Non-monogeneity of Kummer Extensions

Theorem (Smith)

Denote $\mathbb{Q}(\zeta_n, \sqrt[n]{\alpha})$ *by* K*, and suppose there exists a rational prime* ℓ *such that* $\ell \equiv 1 \bmod n$ *and* $\ell < n \cdot \phi(n)$*. Suppose further that* $\alpha \in \mathbb{Z}[\zeta_n]$ *is relatively prime to* ℓ *and that* α *is an* n^{th} *power residue modulo some prime of* $\mathbb{Z}[\zeta_n]$ *above* ℓ*.*

Non-monogeneity of Kummer Extensions

Theorem (Smith)

Denote $\mathbb{Q}(\zeta_n, \sqrt[n]{\alpha})$ *by* K*, and suppose there exists a rational prime* ℓ *such that* $\ell \equiv 1 \bmod n$ *and* $\ell < n \cdot \phi(n)$*. Suppose further that* $\alpha \in \mathbb{Z}[\zeta_n]$ *is relatively prime to* ℓ *and that* α *is an* n^{th} *power residue modulo some prime of* $\mathbb{Z}[\zeta_n]$ *above* ℓ*. Then* K **is not** *monogenic over* $\mathbb{Q}$*.*

Non-monogeneity of Kummer Extensions

Theorem (Smith)

Denote $\mathbb{Q}(\zeta_n, \sqrt[n]{\alpha})$ *by* K*, and suppose there exists a rational prime* ℓ *such that* $\ell \equiv 1 \bmod n$ *and* $\ell < n \cdot \phi(n)$*. Suppose further that* $\alpha \in \mathbb{Z}[\zeta_n]$ *is relatively prime to* ℓ *and that* α *is an* n^{th} *power residue modulo some prime of* $\mathbb{Z}[\zeta_n]$ *above* ℓ*. Then* K **is not** *monogenic over* $\mathbb{Q}$*. Moreover,* ℓ *is an essential discriminant divisor, i.e.,* ℓ *divides* $[\mathcal{O}_K : \mathbb{Z}[\theta]]$ *for every* θ *such that* $\mathbb{Q}(\theta) = K$*.*

Proof Ideas and New Ingredients

Dedekind's Splitting Criterion

Theorem

Let $f(x) \in \mathbb{Z}[x]$ *be monic and irreducible, let* θ *be a root, and let* $L = \mathbb{Q}(\theta)$ *be the number field generated by* θ.

Dedekind's Splitting Criterion

Theorem

Let $f(x) \in \mathbb{Z}[x]$ *be monic and irreducible, let* θ *be a root, and let* $L = \mathbb{Q}(\theta)$ *be the number field generated by* θ*. If* $p \in \mathbb{Z}$ *is a prime that does not divide* $[\mathcal{O}_L : \mathbb{Z}[\theta]]$*, then the factorization of* p *in* $\mathcal{O}_L$ *mirrors the factorization of* $f(x)$ *modulo* p*.*

Dedekind's Splitting Criterion

Theorem

Let $f(x) \in \mathbb{Z}[x]$ be monic and irreducible, let θ be a root, and let $L = \mathbb{Q}(\theta)$ be the number field generated by θ. If $p \in \mathbb{Z}$ is a prime that does not divide $[\mathcal{O}_L : \mathbb{Z}[\theta]]$, then the factorization of p in $\mathcal{O}_L$ mirrors the factorization of $f(x)$ modulo p. That is, if

$$f(x) \equiv \varphi_1(x)^{e_1} \cdots \varphi_r(x)^{e_r} \bmod p$$

is a factorization of $\overline{f(x)}$ into irreducibles in $\mathbb{F}_p[x]$,

Dedekind's Splitting Criterion

Theorem

Let $f(x) \in \mathbb{Z}[x]$ *be monic and irreducible, let* θ *be a root, and let* $L = \mathbb{Q}(\theta)$ *be the number field generated by* θ*. If* $p \in \mathbb{Z}$ *is a prime that does not divide* $[\mathcal{O}_L : \mathbb{Z}[\theta]]$*, then the factorization of* p *in* $\mathcal{O}_L$ *mirrors the factorization of* $f(x)$ *modulo* p*. That is, if*

$$f(x) \equiv \varphi_1(x)^{e_1} \cdots \varphi_r(x)^{e_r} \bmod p$$

is a factorization of $\overline{f(x)}$ *into irreducibles in* $\mathbb{F}_p[x]$*, then* p *factors into primes in* $\mathcal{O}_L$ *as*

$$p = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}.$$

Dedekind's Splitting Criterion

Theorem

Let $f(x) \in \mathbb{Z}[x]$ be monic and irreducible, let θ be a root, and let $L = \mathbb{Q}(\theta)$ be the number field generated by θ. If $p \in \mathbb{Z}$ is a prime that does not divide $[\mathcal{O}_L : \mathbb{Z}[\theta]]$, then the factorization of p in $\mathcal{O}_L$ mirrors the factorization of $f(x)$ modulo p. That is, if

$$f(x) \equiv \varphi_1(x)^{e_1} \cdots \varphi_r(x)^{e_r} \bmod p$$

is a factorization of $\overline{f(x)}$ into irreducibles in $\mathbb{F}_p[x]$, then p factors into primes in $\mathcal{O}_L$ as

$$p = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}.$$

Moreover, the residue class degree of $\mathfrak{p}_i$ is equal to the degree of φ_i.

Dedekind's Index Criterion

Theorem (Dedekind[2])

Let $f(x)$ be a monic, irreducible polynomial in $\mathbb{Z}[x]$, θ a root of f, and $L = \mathbb{Q}(\theta)$.

[2] We employ a generalization due to Kumar and Khanduja.

Dedekind's Index Criterion

Theorem (Dedekind[2])

Let $f(x)$ be a monic, irreducible polynomial in $\mathbb{Z}[x]$, θ a root of f, and $L = \mathbb{Q}(\theta)$. If p is a rational prime, we have

$$f(x) \equiv \prod_{i=1}^{r} f_i(x)^{e_i} \bmod p,$$

where the $f_i(x)$ are monic lifts of the irreducible factors of $\overline{f(x)}$ to $\mathbb{Z}[x]$.

[2] We employ a generalization due to Kumar and Khanduja.

Theorem (Dedekind[2])

Let $f(x)$ be a monic, irreducible polynomial in $\mathbb{Z}[x]$, θ a root of f, and $L = \mathbb{Q}(\theta)$. If p is a rational prime, we have

$$f(x) \equiv \prod_{i=1}^{r} f_i(x)^{e_i} \bmod p,$$

where the $f_i(x)$ are monic lifts of the irreducible factors of $\overline{f(x)}$ to $\mathbb{Z}[x]$. Define

$$d(x) := \frac{f(x) - \prod_{i=1}^{r} f_i(x)^{e_i}}{p}.$$

[2]We employ a generalization due to Kumar and Khanduja.

Theorem (Dedekind[2])

Let $f(x)$ be a monic, irreducible polynomial in $\mathbb{Z}[x]$, θ a root of f, and $L = \mathbb{Q}(\theta)$. If p is a rational prime, we have

$$f(x) \equiv \prod_{i=1}^{r} f_i(x)^{e_i} \bmod p,$$

where the $f_i(x)$ are monic lifts of the irreducible factors of $\overline{f(x)}$ to $\mathbb{Z}[x]$. Define

$$d(x) := \frac{f(x) - \prod_{i=1}^{r} f_i(x)^{e_i}}{p}.$$

Then p divides $[\mathcal{O}_L : \mathbb{Z}[\theta]]$ if and only if $\gcd\left(\overline{f_i(x)}^{e_i - 1}, \overline{d(x)}\right) \neq 1$ for some i, where we are taking the greatest common divisor in $\mathbb{F}_p[x]$.

[2] We employ a generalization due to Kumar and Khanduja.

Relating Monogeneity and Ramification

Lemma (Smith)

Let L be a number field, $f \in \mathcal{O}_L[x]$ a monic, irreducible polynomial, and θ a root of f.

Relating Monogeneity and Ramification

Lemma (Smith)

Let L be a number field, $f \in \mathcal{O}_L[x]$ a monic, irreducible polynomial, and θ a root of f. Let M be a finite extension of L. Suppose that $f(x)$ is irreducible in $M[x]$ and M is unramified over L at all the primes dividing Δ_f.

Relating Monogeneity and Ramification

Lemma (Smith)

Let L be a number field, $f \in \mathcal{O}_L[x]$ a monic, irreducible polynomial, and θ a root of f. Let M be a finite extension of L. Suppose that $f(x)$ is irreducible in $M[x]$ and M is unramified over L at all the primes dividing Δ_f. Then $\mathcal{O}_{L(\theta)} = \mathcal{O}_L[\theta]$ if and only if $\mathcal{O}_{M(\theta)} = \mathcal{O}_M[\theta]$.

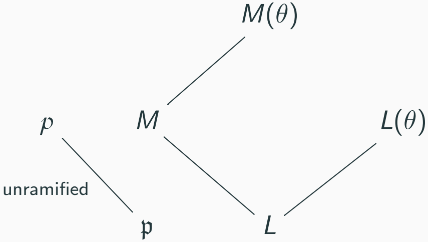
Relating Monogeneity and Ramification

Lemma (Smith)

Let L be a number field, $f \in \mathcal{O}_L[x]$ a monic, irreducible polynomial, and θ a root of f. Let M be a finite extension of L. Suppose that $f(x)$ is irreducible in $M[x]$ and M is unramified over L at all the primes dividing Δ_f. Then $\mathcal{O}_{L(\theta)} = \mathcal{O}_L[\theta]$ if and only if $\mathcal{O}_{M(\theta)} = \mathcal{O}_M[\theta]$.

Idea: Extensions that are unramified at the primes dividing Δ_f don't affect the monogeneity of $f(x)$.

The setup of previous theorem is summarized below.



Further Questions

Further Questions

Can we use monogeneity to recover other arithmetic information about these number fields?

Further Questions

Can we use monogeneity to recover other arithmetic information about these number fields?

Are there further insights from a sheaf-theoretic perspective on these results?

Thank You

Thank you for listening. Please send me an email at hanson.smith@colorado.edu if you have any questions that aren't answered here.

A preprint is available on my website, http://math.colorado.edu/~hwsmith/research.html, and on the arXiv at https://arxiv.org/abs/1909.07184.