Kummer Theory for Number Fields

Antonella Perucca, Pietro Sgobba and Sebastiano Tronto

University of Luxembourg

Benasque, 2019-05-23

Kummer Extensions

- Let K a number field, $G \leq K^{\times}$ torsion-free, $r = \operatorname{rank} G < \infty$.

UNIVERSITÉ DU LUXEMBOURG

Kummer Extensions

- Let K a number field, $G \leq K^\times$ torsion-free, $r = \operatorname{rank} G < \infty$.
- For any M and N with $N \mid M$ consider the extension

$$K\left(\zeta_M, \sqrt[N]{G}\right).$$

Kummer Extensions

- Let K a number field, $G \leq K^\times$ torsion-free, $r = \operatorname{rank} G < \infty$.
- For any M and N with $N \mid M$ consider the extension

$$K\left(\zeta_M, \sqrt[N]{G}\right).$$

- Want to compute $\deg_G(M, N) = \left[K\left(\zeta_M, \sqrt[N]{G}\right) : K\left(\zeta_M\right)\right]$.

UNIVERSITÉ DU LUXEMBOURG

Kummer Extensions

- Let K a number field, $G \leq K^\times$ torsion-free, $r = \operatorname{rank} G < \infty$.
- For any M and N with $N \mid M$ consider the extension

$$K\left(\zeta_M, \sqrt[N]{G}\right).$$

- Want to compute $\deg_G(M, N) = \left[K\left(\zeta_M, \sqrt[N]{G}\right) : K\left(\zeta_M\right)\right]$.
- **Intuition:** $\deg_G(M, N) = N^r$.

UNIVERSITÉ DU LUXEMBOURG

Kummer Extensions

- Let K a number field, $G \leq K^{\times}$ torsion-free, $r = \operatorname{rank} G < \infty$.
- For any M and N with $N \mid M$ consider the extension

$$K\left(\zeta_M, \sqrt[N]{G}\right).$$

- Want to compute $\deg_G(M,N) = \left[K\left(\zeta_M, \sqrt[N]{G}\right) : K\left(\zeta_M\right)\right]$.
- **Intuition:** $\deg_G(M,N) = N^r$.
- **Reality:** $\deg_G(M,N)$ divides N^r.

UNIVERSITÉ DU LUXEMBOURG

Kummer Extensions

Example

Let $K = \mathbb{Q}$, $G = \langle 2^5 \rangle$, $N = M = 5$.
Then $\mathbb{Q}\left(\zeta_5, \sqrt[5]{\langle 2^5 \rangle}\right) = \mathbb{Q}\left(\zeta_5\right)$, so $\deg_G(5,5) = 1$.

Example

Let $K = \mathbb{Q}$, $G = \langle 2^5 \rangle$, $N = M = 5$.
Then $\mathbb{Q}\left(\zeta_5, \sqrt[5]{\langle 2^5 \rangle}\right) = \mathbb{Q}\left(\zeta_5\right)$, so $\deg_G(5,5) = 1$.

Example

Let $K = \mathbb{Q}$, $G = \langle 3, 5 \rangle$, $N = 2$, $M = 10$.
Since $\sqrt{5} \in \mathbb{Q}\left(\zeta_{10}\right)$, we have $\mathbb{Q}\left(\zeta_{10}, \sqrt[2]{\langle 3, 5 \rangle}\right) = \mathbb{Q}\left(\zeta_{10}, \sqrt{3}\right)$, so $\deg_G(2,10) = \left[\mathbb{Q}\left(\zeta_{10}, \sqrt{3}\right) : \mathbb{Q}\left(\zeta_{10}\right)\right] = 2$.

Failure of Maximality

Definition

The **failure of maximality** at (M, N) is

$$C(M,N) := \frac{N^r}{\left[K\left(\zeta_M, \sqrt[N]{G}\right) : K\left(\zeta_M\right)\right]}$$

Failure of Maximality

Definition

The **failure of maximality** at (M, N) is

$$C(M,N) := \frac{N^r}{\left[K\left(\zeta_M, \sqrt[N]{G}\right) : K\left(\zeta_M\right)\right]}$$

Theorem (direct proof in Perucca, Sgobba (2018))

There is a constant $C_0 \geq 1$, depending only on K and G, such that for all integers N, M with $N \mid M$ the integer $C(M, N)$ divides C_0.

Elementary field theory shows

$$C(M,N) =$$

$$= \prod_{\ell \mid N} \underbrace{\frac{\ell^{nr}}{\left[K\left(\zeta_{\ell^n}, \sqrt[\ell^n]{G}\right) : K\left(\zeta_{\ell^n}\right)\right]}}_{A_\ell(N)=C(\ell^n,\ell^n)} \underbrace{\left[K\left(\zeta_{\ell^n}, \sqrt[\ell^n]{G}\right) \cap K\left(\zeta_M\right) : K\left(\zeta_{\ell^n}\right)\right]}_{B_\ell(M,N)}$$

where $n = v_\ell(N)$.

Failure of Maximality

Elementary field theory shows

$$C(M,N) =$$

$$= \prod_{\ell \mid N} \frac{\ell^{nr}}{\underbrace{\left[K\left(\zeta_{\ell^n}, \sqrt[\ell^n]{G}\right) : K(\zeta_{\ell^n})\right]}_{A_\ell(N)=C(\ell^n,\ell^n)}} \underbrace{\left[K\left(\zeta_{\ell^n}, \sqrt[\ell^n]{G}\right) \cap K(\zeta_M) : K(\zeta_{\ell^n})\right]}_{B_\ell(M,N)}$$

where $n = v_\ell(N)$.

Definition

We call $A_\ell(N)$ the **ℓ-adic failure** and $B_\ell(M,N)$ the **ℓ-adelic failure**.

The ℓ-adic Failure $A_\ell(N)$

Theorem (direct proof in Perucca, Sgobba (2018))

There exists a constant α_ℓ, depending only on ℓ, K and G, such that $A_\ell(N) \mid \alpha_\ell$ for all N.
Moreover, $\alpha_\ell = 1$ for all but finitely many primes ℓ.

- For simplicity, let $K = \mathbb{Q}$ and $\ell \neq 2$.

The ℓ-adic Failure $A_\ell(N)$

- For simplicity, let $K = \mathbb{Q}$ and $\ell \neq 2$.
- Let $\mathcal{B} = \{g_1, \ldots, g_r\}$ be a basis for $G \leq \mathbb{Q}^\times$.

UNIVERSITÉ DU LUXEMBOURG

- For simplicity, let $K = \mathbb{Q}$ and $\ell \neq 2$.
- Let $\mathcal{B} = \{g_1, \dots, g_r\}$ be a basis for $G \leq \mathbb{Q}^\times$.
- Write $g_i = b_i^{\ell^{d_i}}$ with $b_i \notin (\mathbb{Q}^\times)^\ell$.

UNIVERSITÉ DU LUXEMBOURG

- For simplicity, let $K = \mathbb{Q}$ and $\ell \neq 2$.
- Let $\mathcal{B} = \{g_1, \dots, g_r\}$ be a basis for $G \leq \mathbb{Q}^\times$.
- Write $g_i = b_i^{\ell^{d_i}}$ with $b_i \notin (\mathbb{Q}^\times)^\ell$.

Theorem (Debry, Perucca (2016))

There exists a basis maximizing $d = \sum d_i$. For all bases maximizing d, the d_i's are the same up to reordering.

UNIVERSITÉ DU LUXEMBOURG

The ℓ-adic Failure $A_\ell(N)$

- We have

$$A_\ell(N) = \ell^s \qquad \text{where } s = \sum_i \min\left(v_\ell(N), d_i\right).$$

UNIVERSITÉ DU LUXEMBOURG

The ℓ-adic Failure $A_\ell(N)$

- We have

$$A_\ell(N) = \ell^s \qquad \text{where } s = \sum_i \min\left(v_\ell(N), d_i\right).$$

- In particular for $v_\ell(N) \geq d_\ell := \max d_i$ we have $s = \sum_i d_i$.

The ℓ-adic Failure $A_\ell(N)$

- We have

$$A_\ell(N) = \ell^s \qquad \text{where } s = \sum_i \min\left(v_\ell(N), d_i\right).$$

- In particular for $v_\ell(N) \geq d_\ell := \max d_i$ we have $s = \sum_i d_i$.
- So $A_\ell(N) = A_\ell(\gcd(N, \ell^{d_\ell}))$.

UNIVERSITÉ DU LUXEMBOURG

$$B_\ell(M,N) = \left[K\left(\zeta_{\ell^n}, \sqrt[\ell^n]{G}\right) \cap K(\zeta_M) : K(\zeta_{\ell^n})\right] \text{ for } n = v_2(N).$$

Theorem (Perucca, Sgobba (2018))

There exists a constant β_ℓ, depending only on ℓ, K and G, such that $B_\ell(M,N) \mid \beta_\ell$ for all M and N.
Moreover, $\beta_\ell = 1$ for all but finitely many primes ℓ (for example when $\zeta_\ell \notin K$).

The ℓ-adelic Failure $B_\ell(M, N)$

- Assume that $K = \mathbb{Q}$ and, for simplicity, that $G \subseteq \mathbb{Q}_{>0}$.

The ℓ-adelic Failure $B_\ell(M, N)$

- Assume that $K = \mathbb{Q}$ and, for simplicity, that $G \subseteq \mathbb{Q}_{>0}$.
- **Problem:** $\sqrt{g} \in \mathbb{Q}(\zeta_d)$ for some d.

UNIVERSITÉ DU LUXEMBOURG

- Assume that $K = \mathbb{Q}$ and, for simplicity, that $G \subseteq \mathbb{Q}_{>0}$.
- **Problem:** $\sqrt{g} \in \mathbb{Q}(\zeta_d)$ for some d.
- The intersection $\mathbb{Q}\left(\zeta_{2^n}, \sqrt[2^n]{G}\right) \cap \mathbb{Q}(\zeta_M)$ equals

$$\mathbb{Q}\left(\zeta_{2^n}, \sqrt{h_1}, \dots, \sqrt{h_s}\right), \quad h_1, \dots, h_s \text{ squarefree integers.}$$

UNIVERSITÉ DU LUXEMBOURG

The ℓ-adelic Failure $B_\ell(M, N)$

- Assume that $K = \mathbb{Q}$ and, for simplicity, that $G \subseteq \mathbb{Q}_{>0}$.
- **Problem:** $\sqrt{g} \in \mathbb{Q}(\zeta_d)$ for some d.
- The intersection $\mathbb{Q}\left(\zeta_{2^n}, \sqrt[2^n]{G}\right) \cap \mathbb{Q}(\zeta_M)$ equals

$$\mathbb{Q}\left(\zeta_{2^n}, \sqrt{h_1}, \ldots, \sqrt{h_s}\right), \quad h_1, \ldots, h_s \text{ squarefree integers.}$$

- We can compute $h_1, \ldots, h_s$, and thus $B_\ell(M, N)$.

UNIVERSITÉ DU LUXEMBOURG

Theorem (Perucca, Sgobba, Tronto (2019))

There are explicitly computable integers M_0 and N_0 such that

$$C(M, N) = C(\gcd(M, M_0), \gcd(N, N_0))$$

for all M and N.

Theorem (Perucca, Sgobba, Tronto (2019))

There are explicitly computable integers M_0 and N_0 such that

$$C(M, N) = C(\gcd(M, M_0), \gcd(N, N_0))$$

for all M and N.

Moreover, there is a **concrete** and **efficient** algorithm to compute these degrees for all M and N.

Effective Results

```
sage: G = [-2^3, (2/3)^27, -1/5]
sage: TotalKummerFailure(G)
M_0 = 120
N_0 = 216

        |  1    2    3    4    5    6    8    10   12   15   20   24   30   40   60   120
  -     -  -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -
  1     |  1    1    1    1    1    1    1    1    1    1    1    1    1    1    1    1
  2     |  1    1    1    1    1    2    2    1    2    1    2    4    2    4    4    8
  3     |  9    9    9    9    9    9    9    9    9    9    9    9    9    9    9    9
  4     |  1    1    1    1    1    1    2    1    2    1    2    4    1    4    4    8
  6     |  9    9    9    9    9    18   18   9    18   9    18   36   18   36   36   72
  8     |  2    2    2    2    2    2    2    2    2    2    2    4    2    4    2    8
  9     |  27   27   27   27   27   27   27   27   27   27   27   27   27   27   27   27
  12    |  9    9    9    9    9    9    18   9    18   9    18   36   9    36   36   72
  18    |  27   27   27   27   27   54   54   27   54   27   54   108  54   108  108  216
  24    |  18   18   18   18   18   18   18   18   18   18   18   36   18   36   18   72
  27    |  81   81   81   81   81   81   81   81   81   81   81   81   81   81   81   81
  36    |  27   27   27   27   27   27   54   27   54   27   54   108  27   108  108  216
  54    |  81   81   81   81   81   162  162  81   162  81   162  324  162  324  324  648
  72    |  54   54   54   54   54   54   54   54   54   54   54   108  54   108  54   216
  108   |  81   81   81   81   81   81   162  81   162  81   162  324  81   324  324  648
  216   |  162  162  162  162  162  162  162  162  162  162  162  324  162  324  162  648
```

Thank you for your attention!