Monogeneity of pure number fields

ALGANT Alumni in China

Khai-Hoan Nguyen-Dang
(Leiden-Padova)
(2019-2021)

Morningside Center of Mathematics, Chinese Academy of Sciences

December 27, 2025

Pure fields and monogeneity: definitions

Let

$$K = \mathbb{Q}(\alpha), \qquad \alpha^n = m \in \mathbb{Z} \setminus \{0\}, \qquad f(x) = x^n - m \text{ irreducible}, \; n \geq 2.$$

Monogeneity vs. α-monogeneity

- K is monogenic if $\exists\, \theta \in \mathcal{O}_K$ with $\mathcal{O}_K = \mathbb{Z}[\theta]$.
- K is α-monogenic if $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

Question

Provide a criterion for m and n so that K is α-monogenic or monogenic.

Main theorem: α-monogeneity criterion

Criterion theorem

Let $K = \mathbb{Q}(\alpha)$ with $\alpha^n = m$ and $x^n - m$ irreducible. Then

$$\mathcal{O}_K = \mathbb{Z}[\alpha] \iff \big(m \text{ is square-free}\big) \text{ and } \nu_p(m^p - m) = 1 \ \ \forall\, p \mid n.$$

Dedekind index theorem

Factor f in $\mathbb{F}_p[X]$ as

$$f(X) = \pi_1(X)^{e_1} \cdots \pi_g(X)^{e_g} \quad (\pi_j \text{ distinct monic irreducibles}).$$

Lift each π_j to a monic $\pi_j \in \mathbb{Z}[X]$ and write

$$f(X) = \pi_1(X)^{e_1} \cdots \pi_g(X)^{e_g} + p\,F(X), \qquad F \in \mathbb{Z}[X].$$

Then

$$p \mid [\mathcal{O}_K : \mathbb{Z}[\alpha]] \iff \exists j \text{ with } e_j \geq 2 \text{ and } \pi_j \mid F \text{ in } \mathbb{F}_p[X].$$

Criterion for α-monogeneity

Only primes $p \mid mn$ can divide $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ (so it suffices to check $p \mid m$ and $p \mid n$).

Case 1: $p \mid m$

Modulo p, $f(X) = X^n - m \equiv X^n$ so $\pi(X) = X$ has multiplicity $e = n \geq 2$. Write

$$f(X) = X^n + pF(X), \qquad F(X) = -\frac{m}{p} \in \mathbb{Z}[X].$$

Dedekind $\Rightarrow$ $p \mid [\mathcal{O}_K : \mathbb{Z}[\alpha]] \iff X \mid F$ in $\mathbb{F}_p[X] \iff F \equiv 0 \pmod{p} \iff p^2 \mid m$. Hence: no such p divides the index $\iff$ m is square-free.

Case 2: $p \mid n$

Write $n = p^r s$ with $(p, s) = 1$ and set $g(X) = X^s - m$. Over $\mathbb{F}_p$,

$$f(X) = X^n - m \equiv (X^s - m)^{p^r} = g(X)^{p^r},$$

so every irreducible factor occurs with multiplicity ≥ 2.

Proof cont.

Case 2: $p \mid n$

Define

$$F(X) = \frac{f(X) - g(X)^{p^r}}{p} \in \mathbb{Z}[X].$$

Since $\bar{f} = \bar{g}^{\,p^r}$, Dedekind's criterion only depends on $\bar{F}$. Let α_0 be a root of g and work in $A = (\mathbb{Z}/p^2\mathbb{Z})[X]/(g)$ where $X^s = m$. Then

$$F(\alpha_0) \equiv \frac{m^{p^r} - m}{p} \pmod{p},$$

so Dedekind $\Rightarrow$ $p \mid [\mathcal{O}_K : \mathbb{Z}[\alpha]] \iff p^2 \mid (m^{p^r} - m)$. Finally, $\nu_p(m^{p^r} - m) = \nu_p(m^p - m)$, so the obstruction is exactly

$$\nu_p(m^p - m) \geq 2 \quad \iff \quad p \mid [\mathcal{O}_K : \mathbb{Z}[\alpha]].$$

Examples

Examples

- $n = 3$: $\mathcal{O}_K = \mathbb{Z}[\alpha]$ iff m square-free and $m \not\equiv \pm 1 \pmod 9$.
- $n = 4$: $\mathcal{O}_K = \mathbb{Z}[\alpha]$ iff m square-free and $m \not\equiv 1 \pmod 4$.
- $n = 5$: $\mathcal{O}_K = \mathbb{Z}[\alpha]$ iff m square-free and $m \not\equiv 1, 7, 18, 24 \pmod{25}$.

Important nuance: cubic case

If $m \equiv \pm 1 \pmod 9$, then $\mathcal{O}_K \neq \mathbb{Z}[\alpha]$ but the field is still monogenic:

$$\theta = \frac{1 \pm \alpha + \alpha^2}{3} \in \mathcal{O}_K, \qquad \mathcal{O}_K = \mathbb{Z}[\theta].$$

Density theorem

Density theorem

Among m with $x^n - m$ irreducible,

$$\delta_n = \lim_{X\to\infty} \frac{\#\{1 \le m \le X : \ \mathcal{O}_K = \mathbb{Z}[\alpha]\}}{X} = \frac{6}{\pi^2} \prod_{p|n} \frac{p}{p+1}.$$

Fix $n \ge 2$. For a prime $p \mid n$ define the "bad" set $E_p = \{m \in \mathbb{Z} : \ m^p \equiv m \pmod{p^2}\}$.

Key local facts

- The congruence $x^p \equiv x \pmod{p^2}$ has exactly p solutions mod p^2: one is 0, the other $(p-1)$ are the Teichmüller lifts in $(\mathbb{Z}/p^2\mathbb{Z})^\times$.
- When intersecting with square-free integers, the class $0 \pmod{p^2}$ disappears automatically. So "bad" square-free classes are exactly the $(p-1)$ Teichmüller unit classes mod p^2.
- Each unit class mod p^2 carries the same square-free density, hence among square-free m we can compute

$$\mathbb{P}(m \in E_p) = \frac{1}{p+1}, \qquad \mathbb{P}(m \notin E_p) = \frac{p}{p+1}.$$

General monogeneity criterion?

- Monogeneity asks for solving an *index form equation* $I(x_2, \ldots, x_n) = \pm 1$ in integers (global Diophantine constraints). Local solubility does not control global solubility.
- Two incompatible phenomena with a purely local criterion:
  1. $\mathbb{Z}[\alpha] \neq \mathcal{O}_K$ but K still monogenic via a different generator (e.g. pure cubics with $m \equiv \pm 1 \pmod 9$).
  2. There exist number fields with *no local obstruction* to being monogenic that are nevertheless *not* monogenic (positive proportion for cubic fields) by L. Alpöge, M. Bhargava, A. Shnidman.

Complementary viewpoints

- Smith studies radical extensions $L(\sqrt[n]{a})/L$. Gives a *relative* criterion for $\sqrt[n]{a}$ to generate a power integral basis over $\mathcal{O}_L$. Specializing to $L = \mathbb{Q}$ recovers exactly our two local conditions.
- Bhargava, Shankar and Wang prove positive density results for maximality of the order $\mathbb{Z}[x]/(f)$ in its fraction field, and for squarefree discriminants for f in a large-dimensional space of monic degree-n polynomials.
- Arpin, Bozlee, Herr and Smith recast monogeneity from a scheme-theoretic perspective.

References

- S. Arpin, S. Bozlee, L. Herr, H. Smith, *The scheme of monogenic generators II: local monogenicity and twists*, Res. Number Theory 9 (2023), 43.
- L. Alpöge, M. Bhargava, A. Shnidman, *A positive proportion of cubic fields are not monogenic yet have no local obstruction to being so*, Math. Ann. (2025).
- M. Bhargava, A. Shankar, X. Wang, *Squarefree values of polynomial discriminants I*, Invent. Math. 228 (2022), 1037–1073.
- M. Bhargava, A. Shankar, X. Wang, *Squarefree values of polynomial discriminants II*, Forum Math. Pi 13 (2025), e17.
- J.-H. Evertse and K. Győry, *Discriminant Equations in Diophantine Number Theory*, Cambridge Univ. Press (2017).
- I. Gaál, *Diophantine Equations and Power Integral Bases*, 2nd ed., Birkhäuser (2019).
- K.-H. Nguyen-Dang and N. T. Hung, *α-monogeneity of pure number fields: criterion and density*, preprint (2025).
- H. Smith, *The monogeneity of radical extensions*, Acta Arith. 198 (2021), 313–327.

Thank you for your attention!
ALGANT FRIEND FOREVER!