Cyclotomic fields

HW1 has been graded for enrolled students. Grades are on Canvas, feedback is in CoCalc.

HW2 has been collected. If you are still planning to submit HW3, please let me know.

Last call for the US election! Election Day is Tuesday, November 3.

Historical interest of cyclotomic fields (part 1)

- Constructibility of regular polygons
- Character theory for finite groups
- Fermat's Last Theorem
- Quadratic and higher reciprocity laws (class field theory)
- Solving trigonometric diophantine equations

$\mathbb{Q}(\zeta_n)$ $\zeta_n = e^{2\pi i/n}$

$[\mathbb{Q}(\zeta_n):\mathbb{Q}] = \varphi(n)$

G	classes
irreps	

→ sums of roots of unity

$$a^n + b^n = c^n \qquad n \geq 3,\ n \text{ odd}$$

in $\mathbb{Q}(\zeta_n)$ $\underbrace{(a+b)(a+\zeta_n b)\cdots(a+\zeta_n^{n-1} b)} = c^n$

Historical interest of cyclotomic fields (part 2)

- Constructibility of regular polygons
- Character theory for finite groups
- Fermat's Last Theorem
- Quadratic and higher reciprocity laws (class field theory)
- Solving trigonometric diophantine equations
- Iwasawa theory

(Conway–Jones 1979)

Q Classify tetrahedra in $\mathbb{R}^3$ (up to similarity) whose dihedral angles are all rational multiples of π.

$$\det(\cos(\theta_{ij}))_{i,j=1}^{4} = 0$$

$$2\cos\theta = e^{i\theta} + e^{-i\theta}$$

Poonen lecture in Number Theory Web Seminar: [recording](), [slides]()

Basic facts about cyclotomic fields

$K = \mathbb{Q}(\zeta_n)$ $\quad n = \text{odd}$ or divisible by 4

(n odd, $\zeta_{2n} \sim -\zeta_n$)

$= \mathbb{Q}[x] / \Phi_n(x)$ $\quad \Phi_n(x) = n\text{-th cyclotomic poly.}$

$[K:\mathbb{Q}] = \varphi(n)$ $\quad x^n - 1 = \prod_{d \mid n} \Phi_d(x)$

$= \prod_{p \mid n} (p-1) p^{e_p - 1}$ $\quad \Phi_n(x) = \prod_{d \mid n} (x^d - 1)^{\mu(n/d)}$

where $n = \prod_p p^{e_p}$ $\quad \mu = \text{Möbius function}$

if $\gcd(n_1, n_2) = 1$, then $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{n_1})\mathbb{Q}(\zeta_{n_2})$ composition

$n = n_1 n_2$ $\quad$ and $\mathbb{Q}(\zeta_{n_1}) \cap \mathbb{Q}(\zeta_{n_2}) = \mathbb{Q}$.

Ring of integers in the prime-power case

$K = \mathbb{Q}(\zeta_n)$

Lemma If $n = p^e$, then $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$

will follow from . . .

Lemma $\lambda := 1 - \zeta_{p^e}$. Then (λ) is prime of norm p (absolute)

and $p\mathcal{O}_K = (\lambda)^{\varphi(n)}$.

Pf $\Phi_n(x) = x^{(p-1)p^{e-1}} + \cdots + x^{p^{e-1}} + 1$

$\Phi_n(1) = p = \prod_{i \in (\mathbb{Z}/n\mathbb{Z})^*} (1 - \zeta_n^i) = \mathrm{Nm}_{K/\mathbb{Q}}(\lambda)$

and $\dfrac{1 - \zeta_n^i}{1 - \zeta_n} \in \mathbb{Z}[\zeta_n]^\times \subseteq \mathcal{O}_K^\times$

$p = \prod_{i \in (\mathbb{Z}/n\mathbb{Z})^*} \lambda \cdot (\text{unit in } \mathcal{O}_K)$

Ring of integers in the prime-power case

<u>Lemma</u> The basis $1, \zeta_n, \dots, \zeta_n^{\varphi(n)-1}$ of $K = \mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$ has discriminant

$$d(1, \zeta_n, \dots, \zeta_n^{\varphi(n)-1}) = \pm p^s \qquad s = p^{e-1}(pe-e-1).$$

<u>Pf</u> $= \pm \prod_{i \neq j} (\zeta_i - \zeta_j) = \prod_{i \in (\mathbb{Z}/n\mathbb{Z})^\times} \Phi_n'(\zeta_n^i) =$ elementary calculation

(reminder: if $P(X) = (X-\alpha_1)\cdots(X-\alpha_n)$
$P'(\alpha_i) = \prod_{j \neq i} (\alpha_i - \alpha_j)$.)

To prove that $\mathbb{Z}[\zeta_n] = \mathcal{O}_K$
- index can only be divisible by powers of p
- control power of p
(case $e=1$ is illustrative)

Ring of integers in the general case

$n =$ general (not 2 mod 4)

Prop For $K = \mathbb{Q}(\zeta_n)$
$\mathcal{O}_K = \mathbb{Z}[\zeta_n]$.

proof n ~~is prime~~ prime power case, (see HW)

to get ~~to~~ general case, $n = p_1^{e_1} \cdots p_r^{e_r}$

$\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{p_1^{e_1}}) \cdots \mathbb{Q}(\zeta_{p_r^{e_r}})$

note that these fields have (pairwise coprime discriminants)

$\Longrightarrow$ get integral basis over $\mathbb{Q}$ by taking products

$\rightarrow$ these are all powers of ζ_n!

$\Longrightarrow \mathcal{O}_K \subseteq \mathbb{Z}[\zeta_n] \subseteq \mathcal{O}_K$

Ramification in cyclotomic fields

($n \not\equiv 2 \bmod 4$)

Corollary: p ramifies in $\mathbb{Q}(\zeta_n) \iff p \mid n$.

Pf Factor $\Phi_n(x)$ over $\mathbb{F}_p$.

(recall: $(x+y)^p = x^p + y^p$) over $\mathbb{F}_p$

Decomposition of primes in cyclotomic fields

For $p \nmid n$, $\qquad K = \mathbb{Q}(\zeta_n)$

$$p\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_r$$

$\operatorname{Norm} \mathfrak{p}_i = p^c \qquad c = \text{order of } p \text{ in } (\mathbb{Z}/n\mathbb{Z})^\times$

(e.g. if $p \equiv 1 \bmod n$, then $\zeta_n \in \mathbb{F}_p^\times$)

Moreover, $\mathrm{Gal}(K/\mathbb{Q})$ acts transitively on $\mathfrak{p}_i$.

(prove a more general theorem later)

The Galois action on primes

The link with quadratic reciprocity

<u>$p \neq q$</u> $p \neq q$ odd primes $\qquad p^* = (-1)^{\frac{p-1}{2}} p$

q splits completely in $\mathbb{Q}(\sqrt{p^*})$ $\qquad \mathbb{Q}(\sqrt{p^*}) \subseteq \mathbb{Q}(\zeta_p)$

$\Updownarrow$ $\qquad$ (Gauss sum)

q splits in $\mathbb{Q}(\zeta_p)$ into an <u>even # of prime ideals</u>

$$\Longrightarrow \left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$