Lecture 16 Prime decomposition and Chebotarev's thm

A number field is a finite field extn $K/\mathbb{Q}$.

Example $K = \mathbb{Q}(\zeta_n)$, with $\zeta_n = e^{2\pi i/n}$, where the dimension of K over $\mathbb{Q}$ is $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$.

Example $K = \mathbb{Q}(\sqrt{D})$, $D \in \mathbb{Z}$, which is of degree 2 if D is not a square.

The ring of integers $\mathcal{O}_K$ of a number field K is the set

$$\mathcal{O}_K := \{ \alpha \in K \mid P_{\alpha/\mathbb{Q}}(X) \in \mathbb{Z}[X] \};$$

this is clearly a ring.

Thm Every non-zero ideal I of $\mathcal{O}_K$ has a decomposition into prime ideals

$$I = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_g^{e_g}$$

which is unique up to a permutation of the indices.

Defn Given a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, its inertia degree is $f_{\mathfrak{p}} := \dim_{\mathbb{F}_p} (\mathcal{O}_K / \mathfrak{p})$ and we have

$$\begin{array}{ccc} \mathcal{O}_K/\mathfrak{p} & \cong & \mathbb{F}_{p^f} \\ | & & | f \\ \mathbb{Z}/p\mathbb{Z} & = & \mathbb{F}_p \end{array}$$

Thm For each prime number p the decomposition

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_g^{e_g}$$

is s.t. $\sum_{i=1}^{g} e_i f_i = [K : \mathbb{Q}]$

For each prime p denote $\tilde{f}(X) \in \mathbb{F}_p[X]$ the effect of

$$\mathbb{Z} \longrightarrow \mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$$
$$a \longmapsto \tilde{a} := a + p\mathbb{Z}$$

on a polynomial $f(X) \in \mathbb{Z}[X]$, i.e. if

$$f(X) = a_0 + a_1 X + \cdots + a_d X^d$$

then

$$\tilde{f}(X) := \tilde{a}_0 + \tilde{a}_1 X + \cdots + \tilde{a}_d X^d.$$

A *lift* of $\phi(X) \in \mathbb{F}_p[X]$ is any $f(X) \in \mathbb{Z}[X]$ s.t. $\tilde{f} = \phi$.

Fix a prime number p.

Prop' Suppose $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Then the decomposition of $\tilde{P}_{\alpha/\mathbb{Q}}(X)$ into monic irreducible factors is of the form

$$\tilde{P}_{\alpha/\mathbb{Q}}(X) = \phi_1(X)^{e_1} \cdot \ldots \cdot \phi_g(X)^{e_g}, \qquad / \mathbb{F}_p$$

where $e_1, \ldots, e_g$ are as above. Moreover,

$$p_i = p\mathcal{O}_K + f_i(\alpha)\mathcal{O}_K,$$

where f_i is any lift of ϕ_i to $\mathbb{Z}[X]$.

Proof — sketch

We have isomorphisms

$$\mathcal{O}_K / p\mathcal{O}_K \cong \mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \cong \frac{\mathbb{Z}[X]/\gamma_{\alpha/\mathbb{Q}}(X)\,\mathbb{Z}[X]}{p\left(\mathbb{Z}[X]/\gamma_{\alpha/\mathbb{Q}}(X)\,\mathbb{Z}[X]\right)}$$

$$\cong \mathbb{Z}[X]/\langle p, \gamma_{\alpha/\mathbb{Q}}(X)\rangle \cong \mathbb{F}_p[X]/\tilde{\gamma}_{\alpha/\mathbb{Q}}(X)\,\mathbb{F}_p[X]$$

$$\cong \mathbb{F}_p[X]/\phi_1(X)^{e_1}\mathbb{F}_p[X] \times \dots \times \mathbb{F}_p[X]/\phi_g(X)^{e_g}\mathbb{F}_p[X]$$

□

As a preparation for Chebotarev's thm, consider the polynomial

$$f(X) = X^4 - X - 1 \in \mathbb{Z}[X].$$

With the help of Pari-GP we may see that it is irreducible over $\mathbb{Q}$, that its Galois group is S_4, and that its discriminant is

$$\Delta_f = -283.$$

Let's take for granted that the factorization into irred's

$$\tilde{f}(X) = \phi_1^{e_1} \cdot \ldots \cdot \phi_g^{e_g} \quad / \mathbb{F}_p$$

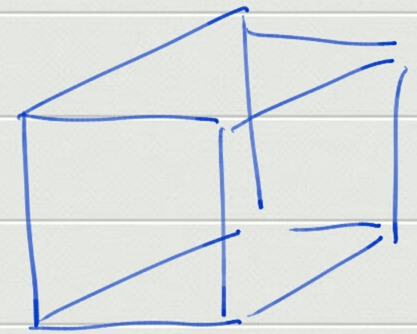
is s.t. $e_1 = \ldots = e_g = 1 \iff p \nmid \Delta_f$.

In the range $p < 7933$ s.t. $p \nmid \Delta_f$ there are 1000 primes,

which distribute as

			partition of 4	$\frac{|C|}{|H|}$
258	primes p	s.t. $\tilde{f}(X)$	has fact. pattern	4	$\frac{6}{24} = \frac{1}{4}$
337	"	"	"	$1+3$	$\frac{8}{24} = \frac{1}{3}$
117	"	"	"	$2+2$	$\frac{3}{24} = \frac{1}{8}$
253	"	"	"	$1+1+2$	$\frac{6}{24} = \frac{1}{4}$
35	"	"	"	$1+1+1+1$	$\frac{1}{24}$

Here C denotes the conjugacy class of $\pi \in S_4$, which may be obtained with the help of the geometric picture of S_4 as the symmetry group of the hexahedron



Recall that there is a $1-1$ correspondence between conjugacy classes of S_n and partitions

$$n = \lambda_1 + \dots + \lambda_s, \qquad (\lambda_1 \leq \dots \leq \lambda_s.)$$

Question Given a polynomial $f(X) \in \mathbb{Z}[X]$, among the factorization patterns of $\tilde{f}(X)$, how often each occur?

We will be able to obtain an answer to this question with the help of Chebotarev's density theorem.

Def'n If S is a set of primes, the density of S is

$$d(S) := \lim_{x \to \infty} \frac{\#\{p \text{ prime} \mid p \leq x, p \in S\}}{\#\{p \text{ prime} \mid p \leq x\}}.$$

Recall that $\forall$ prime number p we have

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_g^{e_g}$$

We say that p splits completely if $g = d$.

Assume for simplicity that $K/\mathbb{Q}$ is Galois.

Thm (Chebotarev) The number of primes p that split completely has density $\frac{1}{d}$, where $d = [K:\mathbb{Q}]$.

Remark Dirichlet's thm states that $\forall\, n \in \{2, 3, \dots\}$ and $a \in \mathbb{Z}$ s.t. $(a, n) = 1$ the proportion of primes p s.t.

$$p \equiv a \pmod{n}$$

is asymptotic to $\frac{1}{\varphi(n)}$. Recall that $K = \mathbb{Q}(\zeta_n)$ has degree $\varphi(n)$ ...