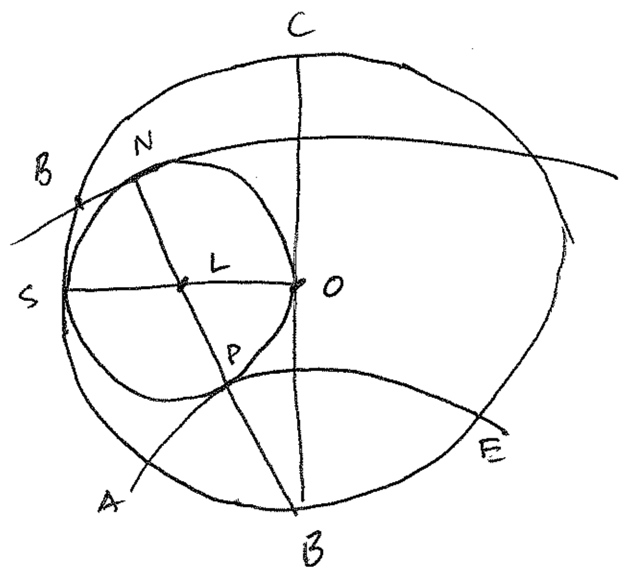
24.1.

A geometry question.



$SL = LO$

Find $\angle BAE$.

Hint.

Theorem. (Kronecker – Weber)

Let $K/\mathbb{Q}$ be Galois with abelian Galois group. Then $K \subseteq \mathbb{Q}(\zeta_n)$ for some n.

24.2. Cyclotomic fields.

Let $\zeta_n = e^{2\pi i/n}$, a primitive root of unity.

Def. $\mathbb{Q}(\zeta_n)$ is called the nth cyclotomic field.

Note that $\mathbb{Q}(\zeta_n) = \mathbb{Q}(x) / (x^n - 1)$

?note: not irreducible

All the roots are roots of unity and $\mathbb{Q}(\zeta_n)$ contains them all. So $\mathbb{Q}(\zeta_n)$ is the splitting field of $x^n - 1$. (it's Galois)

The group of nth roots of unity $\mu_n \subseteq \mathbb{Q}(\zeta_n)$

(it is a group)

A root of unity ζ_n^a is primitive if $(a, n) = 1$.

(If it is not an mth root of unity for some $m | n$)

Def. The nth cyclotomic polynomial is

$$\Phi_n(x) = \prod_{a \in (\mathbb{Z}/n)^\times} (x - \zeta_n^a).$$

Therefore $x^n - 1 = \prod_{d|n} \Phi_d(n)$.

(i.e. if $n = p$, $\Phi_p(n) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \dots + 1$.

By Möbius inversion, $\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}$.

$\Phi_1(x) = x - 1$

$\Phi_2(x) = x + 1$

$\Phi_3(x) = x^2 + x + 1$

$\Phi_4(x) = x^2 + 1$

$\Phi_5(x) = x^2 - x + 1$

Compute. For all $n \leq 100$, all coeffs are 0 or ± 1.

Is it always true?

Theorem.

(1) $\Phi_n(x)$ is irreducible,

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

(3) $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ acts ~~primitively~~ transitively on the primitive nth roots of 1

(4) The map $a \longrightarrow (\zeta_n \to \zeta_n^a)$ induces an isomorphism $(\mathbb{Z}/n)^\times \longrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$.
← mumble something about Artin L-functions!

Proof. Look at $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$.
Any $\sigma \in G$ must send ζ_n to ζ_n^a for some a with $(a,n)=1$.

Indeed, any ~~an~~ embedding $\mathbb{Q}(\zeta_n) \hookrightarrow \mathbb{C}$ must do so.
Moreover, σ is determined by its action on ζ_n.

So get a map $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \longrightarrow (\mathbb{Z}/n)$
image in fact in $(\mathbb{Z}/n)^\times$
is injective, and surjective because any $\zeta_n \to \zeta_n^a$ is an automorphism.

Gives (4) and (3). Also, it's a group hom $\zeta_n \to \zeta_n^a \to (\zeta_n^a)^b$ same as $\zeta_n \to \zeta_n^{ab}$.

(2) follows (define $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$)

(1) follows because $\Phi_n(x) = \prod_{\sigma \in G} (x - \sigma(\zeta_n))$.

Proposition. Let $n = p^r$, $K = \mathbb{Q}(\zeta_n)$, $\pi = 1 - \zeta_n$. Then:

(1) The ideal (π) of $\mathcal{O}_K$ is prime of residue class degree 1. $p\mathcal{O}_K = (\pi)^e$ where $e = \varphi(p^r) = p^{r-1}(p-1) = [K:\mathbb{Q}]$.

(2) $\mathrm{Disc}(\mathbb{Z}[\zeta_{p^r}]/\mathbb{Z}) = \mathrm{Disc}(1, \zeta_{p^r}, \zeta_{p^r}^2, \ldots, \zeta_{p^r}^{e-1}) = \pm p^s$, where $s = p^{r-1}(pr - r - 1)$.

(3) $\mathcal{O}_K = \mathbb{Z}[\zeta_{p^r}]$.

Proof. (1).

The cyclotomic polynomial is

$$\Phi_{p^r}(x) = \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1} = x^{p^{r-1}(p-1)} + \cdots + x^{p^{r-1}} + 1.$$

Plug in $x = 1$. $\quad p = \prod_{a \in (\mathbb{Z}/p^r)^\times} (1 - \zeta_{p^r}^a)$.

That's cool!

Now, $\dfrac{1 - \zeta_{p^r}^a}{1 - \zeta_{p^r}}$ is an algebraic integer, $1 + \zeta_{p^r} + \cdots + \zeta_{p^r}^{a-1}$.

But $\dfrac{1 - \zeta_{p^r}}{1 - \zeta_{p^r}^a}$ is also an algebraic integer because $\zeta_{p^r} = \zeta_{p^r}^{a\bar{a}}$ ($\bar{a}$: inverse of a mod n)

namely, $1 + \zeta_{p^r}^a + \cdots \zeta_{p^r}^{a \cdot (\bar{a} - 1)}$

and so the quotient is in $\mathcal{O}_K^\times$.

Can write $p = \prod_{a \in (\mathbb{Z}/p^r)^\times} (1 - \zeta_p) \cdot (\text{some unit})$

$$= (\text{unit}) \cdot (1 - \zeta_p)^{\varphi(p^r)}.$$

Proves (1). (In combo with efg.)

(2). We have

$$\pm \operatorname{Disc}(1, \zeta_{p^r}, \ldots, \zeta_{p^r}^{\varphi(p^r) - 1}) = \prod_{i \neq j} (\zeta^i - \zeta^j)$$

$$= \prod_i \Phi_n'(\zeta^i)$$

$$= N_{\mathbb{Q}(\zeta_{p^r}) | \mathbb{Q}} \, \Phi_n'(\zeta_{p^r}).$$

24.5.

Now we have $(X^{p^{r-1}} - 1)\,\Phi_{p^r}(x) = X^{p^r} - 1$

Take derivatives:

$$(X^{p^{r-1}} - 1)\,\Phi'_{p^r}(x) + p^{r-1} X^{p^{r-1}-1} \cdot \Phi_{p^r}(x) = p^r X^{p^r - 1}$$

Plug in ζ_{p^r}:

$$(*) \quad (\zeta_p - 1)\,\Phi'_{p^r}(\zeta_{p^r}) = p^r \cdot \zeta_{p^r}^{-1}$$

Take norms down to $\mathbb{Q}$:

$$N_{\mathbb{Q}(\zeta_{p^r})|\mathbb{Q}}(\zeta_{p^r}) = \pm 1.$$

$$N_{\mathbb{Q}(\zeta_{p^r})|\mathbb{Q}}(\zeta_p - 1) = N_{\mathbb{Q}(\zeta_{p^r})|\mathbb{Q}(\zeta_p)}\, N_{\mathbb{Q}(\zeta_p)|\mathbb{Q}}(\zeta_p - 1)$$

$$= N_{\mathbb{Q}(\zeta_{p^r})|\mathbb{Q}(\zeta_p)}(\pm p)$$

$$= \pm p^{p^{r-1}}.$$

So: Taking norms in $(*)$,

$$\pm \cdot p^{p^{r-1}} \cdot N(\Phi'_{p^r}(\zeta_{p^r})) = p^{r(p-1)p^{r-1}}$$

and so $N(\Phi'_{p^r}(\zeta_{p^r})) = \pm p^{p^{r-1}[r(p-1) - 1]}$.

25.1. Cyclotomic fields.

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

Properties.

(1) Galois and abelian $/\mathbb{Q}$,

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/n)^\times$$
$$(\zeta_n \mapsto \zeta_n^a) \longleftarrow\!\!\shortmid\; a.$$

If $n = p^r$:

(2) p is totally ramified, with $(1-\zeta_n)^{\varphi(n)} = (\text{unit}) \cdot p$.

(3) ~~Disc(1, ζ,~~ $\mathrm{Disc}(\mathbb{Z}[\zeta_n]/\mathbb{Z}) = \pm p^s$ with $s = p^{r-1}(pr - r - 1)$.

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

Proof of (4).

By (2), we have (for $\pi := 1 - \zeta_n$)

$$\mathcal{O}_K / \pi\mathcal{O}_K \cong \mathbb{Z}/p.$$

And, $\pi\mathcal{O}_K \cap \mathbb{Z} = (p)$, so $\pi\mathcal{O}_K, 1 + \pi\mathcal{O}_K, \ldots, (p-1) + \pi\mathcal{O}_K$ all distinct.

So: $\mathbb{Z} + \pi\mathcal{O}_K = \mathcal{O}_K$,

and so $\mathbb{Z}[\zeta_n] + \pi\mathcal{O}_K = \mathcal{O}_K$.

Well, $\mathbb{Z}[\zeta_n] + \pi(\mathbb{Z}[\zeta_n] + \pi\mathcal{O}_K) = \mathcal{O}_K$,

$\mathbb{Z}[\zeta_n] + \pi^2\mathcal{O}_K = \mathcal{O}_K$

$\mathbb{Z}[\zeta_n] + \pi^3\mathcal{O}_K = \mathcal{O}_K$ etc.

Eventually the madness must stop.

Indeed, since $\mathrm{Disc}(\mathbb{Z}[\zeta_n])$ is a power of p, so is $[\mathcal{O}_K : \mathbb{Z}[\zeta_n]]$, so $p^m\mathcal{O}_K \subseteq \mathbb{Z}[\zeta_n]$ for m big enough.

So, $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$, we're done.

25.2. General cyclotomic fields.

Theorem.

(1) $[\mathbb{Q}(\zeta_n):\mathbb{Q}] = \varphi(n)$ with $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to (\mathbb{Z}/n)^\times$
(same)

(2) $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$. (new!)

sketch
Proof of (2). Induction on number of primes dividing n.

Let $n = p^r \cdot m$.

Claim. $\mathbb{Q}(\zeta_m) \cdot \mathbb{Q}(\zeta_{p^r}) = \mathbb{Q}(\zeta_n)$.

Proof. $\subseteq$ is clear. For $\supseteq$, $\zeta_m \cdot \zeta_{p^r}$ is a primitive $m \cdot p^r$ th root of unity.
(if $(\zeta_m \cdot \zeta_{p^r})^a = 1$ then $m \mid a$ and $p^r \mid a$).

~~Want to~~
Now, $\mathcal{O}_{\mathbb{Q}(\zeta_n)} \supseteq \mathbb{Z}[\zeta_{p^r}] \cdot \mathbb{Z}[\zeta_m] = \mathbb{Z}[\zeta_{m \cdot p^r}]$.
(the $=$: think about it!)

We conclude with the following lemmas.

Lemma 1. Let L, K be number fields, w/ $[KL:\mathbb{Q}] = [K:\mathbb{Q}][L:\mathbb{Q}]$.
(i.e. $K \cap L = \mathbb{Q}$)

Let $d = \gcd(\Delta_K, \Delta_L)$.
Then, $\mathcal{O}_{KL} \subseteq \frac{1}{d} \mathcal{O}_K \mathcal{O}_L$.

Lemma 2. We have
p ramifies in $\mathbb{Q}(\zeta_m) \longleftrightarrow p \mid m$.

(These, together, show $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$.)

Sketches of proofs:
(1) a little long. more of this linear algebra business.
(2). First of all, if $p \mid m$, p ramifies in $\mathbb{Q}(\zeta_p)$ so certainly in $\mathbb{Q}(\zeta_m)$.

For the other direction, argue $\Delta := \mathrm{Disc}(\mathbb{Q}(\zeta_m)) \mid m^{\varphi(m)}$.

We know $\Delta \mid \mathrm{Disc}(\mathbb{Z}[\zeta_m]/\mathbb{Z}) = N_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(\Phi_m'(\zeta_m))$.

Let $x^m - 1 = \Phi_m(x) \cdot g(x)$ for some $g(x) \in \mathbb{Z}[x]$

$$m x^{m-1} = \Phi_m'(x) \cdot g(x) + \Phi_m(x) g'(x)$$

Plugging in $x = \zeta_m$, $\quad m \cdot \zeta_m^{-1} = \Phi_m'(\zeta_m) \cdot g(\zeta_m) + 0$

Taking norms, $\quad m^{\varphi(m)} = N_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(\Phi_m'(\zeta_m)) \cdot \underbrace{N_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(g(\zeta_m))}_{\text{some integer}}$

and so done.

<u>The decomposition of primes</u>.

<u>Theorem</u>. Let $K = \mathbb{Q}(\zeta_n)$. Write $n = \prod_p p^{r_p}$.
Fix p and write $m = n/p^{r_p}$. (Includes the case $r_p = 0$, $m = n$.)
Let (*) $f(p)$ = smallest number with $p^{f(p)} \equiv 1 \pmod m$.
(<u>index of p mod m</u>)
(order of p in $(\mathbb{Z}/m)^\times$.)

Then, $p\mathcal{O}_K = (\mathfrak{p}_1 \cdots \mathfrak{p}_g)^{\varphi(p^{r_p})}$,
where $g = \varphi(m)/f(p)$,
residue class of each prime is $f(p)$.

<u>Remark</u>. Expresses Lemma 2.
$\varphi(p^{r_p}) > 1 \longleftrightarrow p$ ramifies in $K \longleftrightarrow r_p > 0$.
(<u>exception</u>: if $p = 2$, $r_p > 1$.)

(25.4) = 26.2

Some interesting numerical data.

$n = 7$: $f(1) = 1$, $f(2) = 3$, $f(3) = 6$, $f(4) = 3$, $f(5) = 6$, $f(6) = 2$

($f(3)$, $f(5)$: primitive roots.)

$7\mathcal{O}_K = \mathfrak{p}^6$. $\varphi(7) = 6$.

$p \equiv 1 \pmod 7$: p splits completely in K.

$p \equiv 6 \pmod 7$: $p = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3$ with $f(\mathfrak{p}_i | p) = 2$.

$p \equiv 2, 4 \pmod 7$: $p = \mathfrak{p}_1 \cdot \mathfrak{p}_2$ with $f(\mathfrak{p}_i | p) = 3$.

Ex. $n = 20$.

$2\mathcal{O}_K = \mathfrak{p}^{\varphi(4)} = \mathfrak{p}^2$. Here 2 has order 4 in $(\mathbb{Z}/5)^\times$. $f(\mathfrak{p}|2) = 4$.

$5\mathcal{O}_K = (\mathfrak{p}_1 \cdot \mathfrak{p}_2)^4$ $f(\mathfrak{p}_i | 5) = 1$ because 5 has order 1 in $(\mathbb{Z}/4)^\times$.

First consider the unramified case: suppose $p \nmid n$, $m = n$.

Choose any prime $\mathfrak{p}$ lying over p.

Consider the extension $[\mathcal{O}_K/\mathfrak{p} : \mathbb{Z}/p]$ of degree f.

Prove $f = f(p)$.

This is a Galois extension, cyclic, generated by the Frobenius map $\mathrm{Frob}(p) = \{a \longrightarrow a^p\}$.

Write $\tau = \mathrm{Frob}(p)$.

Claim. $\tau^k = id \longleftrightarrow p^k \equiv 1 \pmod n$.

(Note that the smallest k with $\tau^k = id$ is $f = [\mathcal{O}_K/\mathfrak{p} : \mathbb{Z}/p] = 1$.)

$\longleftarrow$: If $p^k \equiv 1 \mod n$, then $\zeta_n^{p^k} = \zeta_n$.

Acts trivially on $\mathbb{Z}[\zeta_n]/\mathfrak{p}$.

25.5. = 26.3. If $\tau^k = id$, then $\zeta_n^{p^k} - \zeta_n \in \mathfrak{p}$.

Writing $p^k \equiv b \pmod n$ with $1 \le b \le n$,

$$\zeta_n \equiv \zeta_n^b \pmod{\mathfrak{p}}, \text{ so}$$

$$1 \equiv \zeta_n^{b-1} \pmod{\mathfrak{p}}. \qquad (*)$$

Now $\prod_{j=1}^{n-1} (x - \zeta_n^j) = \frac{x^n - 1}{x - 1} = x^{n-1} + \cdots + 1$

so $\prod_{j=1}^{n-1} (1 - \zeta_n^j) = n$.

Suppose $b > 1$, then the left is $0 \bmod \mathfrak{p}$

the right is not, contradiction, $b = 1$.

Therefore: Every $\mathfrak{p} | p$ has residue class degree $f(p)$ and there are $\varphi(n)/f(p)$ of them, as desired.

In fact, the following is true.

Theorem. Given $\mathfrak{p} | p$ as above. Then there exists a unique element $\sigma \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ such that:

(1) $\sigma(\mathfrak{p}) = \mathfrak{p}$,

(2) For all $a \in \mathcal{O}_K$, $\sigma(a) \equiv a^p \bmod \mathfrak{p}$,

(2') Regarded as an automorphism of $\mathbb{Z}[\zeta_n]/\mathfrak{p}$ which fixes $\mathbb{Z}/(p)$, i.e. as an element of

$$Gal(\mathbb{Z}[\zeta_n]/\mathfrak{p} \mid \mathbb{Z}/(p)),$$

it is the Frobenius map $\{a \to a^p\}$.

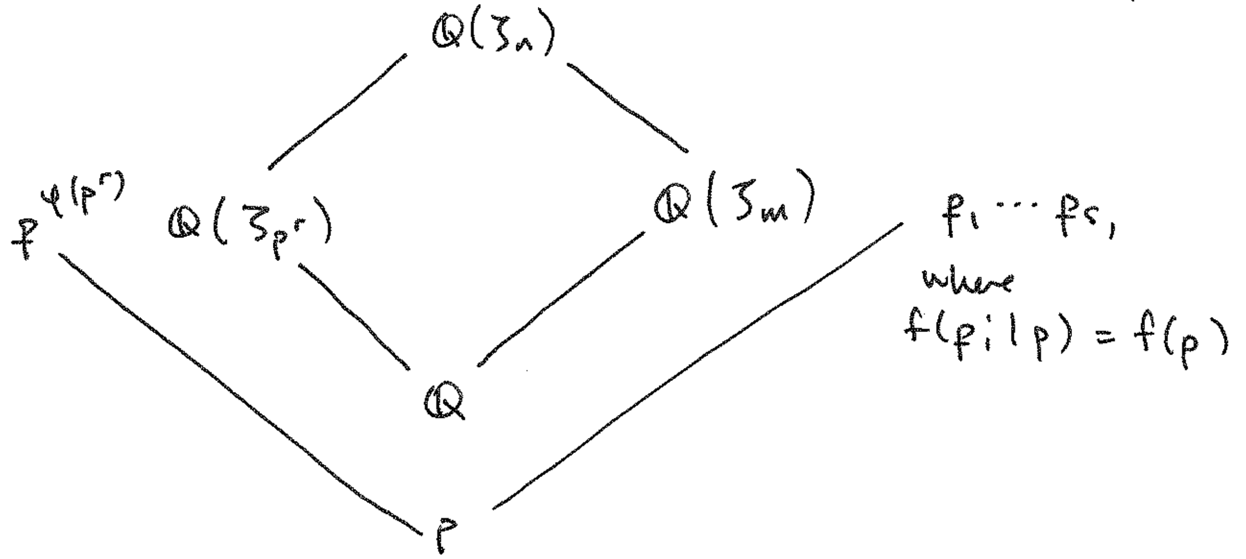
This is called the (global) Frobenius automorphism at $\mathfrak{p}$,

$$\left(\frac{\mathbb{Q}(\zeta_n)/\mathbb{Q}}{\mathfrak{p}}\right).$$

The ramified case.

Suppose $p | n$ and $n = p^{r_p} \cdot m$. Write $r = r_p$.

We have



Suppose $\mathfrak{P}_i$ in $\mathbb{Q}(\zeta_n)$ lies over $\mathfrak{p}_i$.

(∗) Then $f(\mathfrak{P}_i | p) \geq f_p$ (res. class degree)

$e(\mathfrak{P}_i | p) \geq \varphi(p^r)$ (ramification index)

But this takes up all the room!

Since $\displaystyle\sum_{i=1}^{s} \varphi(p^r) \cdot f(p) = \varphi(p^r) \cdot f(p) \frac{\varphi(m)}{f(p)} = \varphi(p^r)\varphi(m) = \varphi(n)$,

we conclude $\mathfrak{P}_i$ is the only prime ideal above $\mathfrak{p}_i$, and

(∗) are equalities.

So, $p\mathcal{O}_{\mathbb{Q}[\zeta_n]} = (\mathfrak{P}_1 \cdots \mathfrak{P}_s)^{\varphi(p^r)}$, q.e.d.

Lamé and Kummer, on Fermat's Last Theorem.

Fermat's last theorem. Let $n > 2$. Then the equation
$$X^n + Y^n = Z^n$$
only has solutions with $X, Y,$ or Z equal to 0.

(Proved: Wiles, Taylor-Wiles)

(Note: False for $n = 2$)

First reduction. Enough to take $n = p$ prime (clear).
Second reduction. $X, Y,$ and Z are all coprime.

Theorem. (Kummer) If $p \nmid h(\mathbb{Q}(\zeta_p))$, then FLT is true for exponent p.

Will prove: "First case of FLT":

Thm. If $p \nmid h(\mathbb{Q}(\zeta_p))$, then $X^p + Y^p = Z^p$ $(p > 2)$ does not have any solutions with p coprime to XYZ.

Same idea is behind the wrong proof:

factor in $\mathbb{Q}(\zeta_p)$. Get $\prod_{i=0}^{p-1} (X + \zeta_p^i Y) = Z^p$.

If we had unique factorization,

- prove all the $X + \zeta_p^i Y$ are coprime
- hence, the $X + \zeta_p^i Y$ are all pth powers
- push for a contradiction.

We'll see that Kummer's condition saves the proof.

Lemma. All the $X + \zeta_p^i Y$ are coprime.

Proof. If $\mathfrak{q}$ is a prime dividing $X + \zeta_p^i y$
and $X + \zeta_p^j y$

then it divides $(\zeta_p^j - \zeta_p^i) y$.

Now $(\zeta_p^j - \zeta_p^i) = (\zeta_p^{j-i} - 1) = (\zeta_p - 1) = \mathfrak{p}$
the unique prime ideal of $\mathbb{Q}(\zeta_p)$ above p.

So $\mathfrak{q} \mid \mathfrak{p} \cdot y$.

Similarly $\mathfrak{q}$ divides ~~$x\zeta_p^{-i} + y$~~ $X \cdot \zeta_p^{-i} + y$
and ~~$x\zeta_p^{-j}$~~ $X \cdot \zeta_p^{-j} + y$

hence $(\zeta_p^{-i} - \zeta_p^{-j}) X$, which as an ideal is $\mathfrak{p} \cdot x$.

Since x, y coprime, $\mathfrak{q} \mid \mathfrak{p}$ and so $\mathfrak{q} = \mathfrak{p}$.

So, $\mathfrak{p}$ divides all the $X + \zeta_p^i y$ in particular $x + y$
which is an integer.

So $p \mid x + y$

$p \mid (x+y)^p \equiv x^p + y^p = z^p$

So $p \mid z$ (contradiction.)

Theorem. ("First case of FLT")

If $p \nmid h(\mathbb{Q}(\zeta_p))$ ~~or~~ then $x^p + y^p = z^p$ $(p > 2)$
has no solutions with p coprime to xyz.

Proof. Factor in $\mathbb{Q}(\zeta_p)$ $\prod_{i=0}^{p-1} (x + \zeta_p^i y) = z^p$.

Lemma. All the $x + \zeta_p^i y$ are coprime. (unless $p \mid z$)
(Proved last time)

Lemma. If $\alpha \in \mathbb{Z}[\zeta_p]$, then $\alpha^p \in \mathbb{Z} + p\mathbb{Z}[\zeta_p]$.

Proof. Write $\alpha = a_0 + a_1 \zeta_p + a_2 \zeta_p^2 + \cdots + a_{p-2} \zeta_p^{p-2}$

By the "Freshman Binomial Theorem",

$$\alpha^p \equiv a_0^p + (a_1 \zeta_p)^p + \cdots + (a_{p-2} \zeta_p^{p-2})^p \pmod p$$
$$\equiv a_0^p + a_1^p + \cdots + a_{p-2}^p \pmod p.$$

↑ Here, mod p means mod $p\mathbb{Z}[\zeta_p]$.

Lemma. Let $\alpha = a_0 + a_1 \zeta_p + a_2 \zeta_p^2 + \cdots + a_{p-1} \zeta_p^{p-1}$
with $a_i \in \mathbb{Z}$, at least one a_i is 0.
If α is divisible by an integer n (i.e. if $\alpha \in n\mathbb{Z}[\zeta_p]$)
then each a_i is divisible by n.

Proof. The remaining elements (choose any $p-1$ ζ_p^i's)
form a basis for $\mathbb{Z}[\zeta_p]$, because $1 + \zeta_p + \cdots + \zeta_p^{p-1} = 0$.
So, the result is clear.

Proof of theorem.

Look at $\prod_{i=0}^{p-1} (x + \zeta_p^i y)$ as an equality of ideals.

Now, each ideal on left is a pth power.

(→)

27.2. Write $(x+\zeta_p^i y) = \mathfrak{a}_i^p$ for some $\mathfrak{a}_i$.

$\mathfrak{a}_i$ is also principal because $p \nmid h(\mathbb{Q}(\zeta_p))$.

Say, $\mathfrak{a}_i = (\alpha_i)$.

Take $i=1$, write $\alpha = \alpha_1$. $x + \zeta_p y = u\alpha^p$ for some unit.

We can write $u = \zeta_p^r \cdot v$ with $v = \bar{v}$. (Sorry! Omitting proof. See Milne 101-102.)

Also, $\alpha^p \equiv a \pmod p$ for some $a \in \mathbb{Z}$.

So $x + \zeta_p y = u\alpha^p = \zeta_p^r v \alpha^p \equiv \zeta_p^r v a \pmod p$

$x + \zeta_p^{-1} y = \quad \cdots \quad \equiv \zeta_p^{-r} v a \pmod p$

and so $\zeta_p^{-r}(x + \zeta_p y) \equiv \zeta_p^r (x + \zeta_p^{-1} y)$.

So, FOILing, $x + \zeta_p y - \zeta_p^{2r} x - \zeta_p^{2r-1} y \equiv 0 \mod p$.

If these roots of unity are all distinct, then p divides x and y.

(Contradiction)

Therefore, one of the following is true.

(0) $p = 3$. (work out separately: Milne, p. 103)

(1) $\zeta_p^{2r} = 1$, but then $\zeta_p y - \zeta_p^{-1} y \equiv 0 \mod p$,

so $p \mid y$.

(2) $\zeta_p^{2r-1} = 1$, $\zeta_p = \zeta_p^{2r}$, so

$(x-y) - (x-y)\zeta_p \equiv 0 \pmod p$,

so $p \mid x - y$.

Can rule this out from the beginning!

$x^p + y^p = z^p \longrightarrow x^p + (-z)^p = (-y)^p$

$p \mid x - y \Rightarrow x \equiv y \mod p$. If $x \equiv y \mod p$,

$x \equiv -z \mod p$

Get $x^p + x^p \equiv -x^p \mod p$.

So $p \mid x$.

(3) $\zeta_p^{2r-1} = \zeta_p$, i.e. $\zeta_p^{2r-2} = 1$, but then

$$x - \zeta_p^2 x \equiv 0 \pmod p$$

and again $p \mid x$.

Galois theory and prime decomposition.

Given an extension $K/\mathbb{Q}$, Galois (or L/K, everything works) with $G = \mathrm{Gal}(K/\mathbb{Q})$.

$\mathfrak{p} \subseteq \mathcal{O}_K$ prime over p.

Proposition. $G = \mathrm{Gal}(K/\mathbb{Q})$ acts transitively on the primes over p.

Proof 1. Assume $\mathfrak{p}, \mathfrak{p}'$ are two such primes but no $\sigma \in G$ exists with $\sigma(\mathfrak{p}) = \mathfrak{p}'$.

Find, by CRT, $x \in \mathcal{O}_K$ with $x \equiv 0 \pmod{\mathfrak{p}'}$

$x \equiv 1 \pmod{\sigma(\mathfrak{p})}$ for all $\sigma(\mathfrak{p})$.

Take norms: $N_{K/\mathbb{Q}}(x) = \prod_{\sigma \in G} \sigma(x) = x \cdot \prod_{\sigma \neq 1} \sigma(x) \in \mathfrak{p}'$.

So it is in $\mathfrak{p}' \cap \mathbb{Z} = (p)$.

But, we can see, $N(x) = \prod_{\sigma \in G} \sigma(x)$ is not in $\mathfrak{p}$.

A good way to prove this: $x \equiv 1 \pmod{\sigma(\mathfrak{p})}$

$\Updownarrow$

$\sigma^{-1}(x) \equiv \sigma^{-1}(1) \pmod{\mathfrak{p}}$

$\sigma^{-1}(x) \equiv 1 \pmod{\mathfrak{p}}$

so $\sigma^{-1}(x) \notin \mathfrak{p}$.

and, $N(x) = \prod_{\sigma \in G} \sigma(x) = \prod_{\sigma \in G} \sigma^{-1}(x) \notin \mathfrak{p}$ by primality.

So it's not in (p), Contradiction.

~~Proof 2~~.

27.4. **Cor.** If $\mathfrak{p}, \mathfrak{p}'$ lie over p then

$$e(\mathfrak{p}|p) = e(\mathfrak{p}'|p)$$
$$f(\mathfrak{p}|p) = f(\mathfrak{p}'|p).$$

Proof. For some $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$,

$$\sigma: \quad K \longrightarrow K, \quad \mathcal{O}_K \longrightarrow \mathcal{O}_K, \quad \mathfrak{p} \longrightarrow \mathfrak{p}'$$

is an isomorphism.

In this case the efg theorem is just $efg = [K:\mathbb{Q}]$.

Def. If $K/\mathbb{Q}$ is Galois with $\mathfrak{p}|p$, the <u>decomposition group</u> is

$$D_\mathfrak{p} := \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) : \sigma(\mathfrak{p}) = \mathfrak{p}\}.$$

Stabilizer of Galois action on primes above $\mathfrak{p}$.

By group theory:

(1) All the groups $D_\mathfrak{p}$ are <u>conjugate</u>:
If $\tau(\mathfrak{p}) = \mathfrak{p}'$,
then $\sigma(\mathfrak{p}) = \mathfrak{p} \longleftrightarrow \tau\sigma\tau^{-1}(\mathfrak{p}') = \mathfrak{p}'$.

(2) size of Galois orbit on primes
$= \#$ of primes over p $= \dfrac{\#G}{\# D_\mathfrak{p}}$

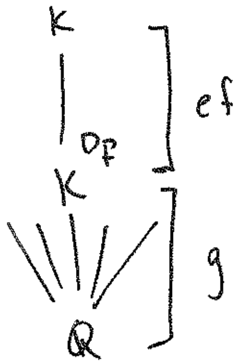
and so $\# D_\mathfrak{p} = \dfrac{\#G}{g} = \dfrac{efg}{g} = ef$.

~~Write $K^{D_\mathfrak{p}}$ for the fixed field.~~

If $\# D_\mathfrak{p} = [K:\mathbb{Q}]$, no splitting.
If also no ramification, p is totally inert.
If unramified and $D_\mathfrak{p} = 1$, then totally split.

27.5. The picture (version 1).

Let $K^{D_\mathfrak{p}}$ = fixed field of decomp group.



Prop. In this diagram, let $\mathfrak{p}_D$ be the prime of $K^{D_\mathfrak{p}}$ below $\mathfrak{p}$.

Then,

(1) $\mathfrak{p}$ is the only prime of K above $\mathfrak{p}_D$,

(2) The ramification index and residue class degrees of $\mathfrak{p}_D$ over p are equal to 1.

Proof. (1) $\mathrm{Gal}(K/K^{D_\mathfrak{p}})$ acts transitively on the primes of K over $K^{D_\mathfrak{p}}$. But it fixes $\mathfrak{p}$.

So that means $e(\mathfrak{p}|\mathfrak{p}_D) \cdot f(\mathfrak{p}|\mathfrak{p}_D) = [K : K^{D_\mathfrak{p}}] = ef$.

So $e(\mathfrak{p}|\mathfrak{p}_D) = e(\mathfrak{p}|p)$.

But $e(\mathfrak{p}|p) = e(\mathfrak{p}|\mathfrak{p}_D)\, e(\mathfrak{p}_D|p)$, so $e(\mathfrak{p}_D|p) = 1$.

Similarly $f(\mathfrak{p}_D|p) = 1$

~~and therefore $g(K^{D_\mathfrak{p}}/\mathbb{Q}) = g$.~~

Next time: Get a surjection

$$D_\mathfrak{p} \longrightarrow \mathrm{Gal}(\mathcal{O}_K/\mathfrak{p} \mid \mathbb{Z}/p\mathbb{Z}).$$

28.2. Consider the ~~surject~~ homomorphism

$$D_{\mathfrak{p}} \longrightarrow \mathrm{Gal}\left(\mathcal{O}_K/\mathfrak{p} \,\middle|\, \mathbb{Z}/p\mathbb{Z}\right)$$

$$\sigma \longrightarrow \left(a + \mathfrak{p} \longrightarrow \sigma(a) + \mathfrak{p}\right).$$

Well-defined, because σ fixes $\mathfrak{p}$
(and the identity homomorphism fixes $\mathbb{Z}$).

<u>Theorem</u>. The map is surjective.

<u>Proof</u>. First consider the following reduction.

$$\begin{array}{cc} K & \mathfrak{p} \\ | & | \\ K^{D_{\mathfrak{p}}} & \mathfrak{p}_D \\ | & | \\ \mathbb{Q} & p \end{array}$$

By previous prop. ~~$e(K^{D_{\mathfrak{p}}} | \mathbb{Q}) = f(K^{D_{\mathfrak{p}}} | \mathbb{Q}) = 1$~~
and $\mathfrak{p}$ is the only prime above $\mathfrak{p}_D$.

This means $\mathrm{Gal}\left(\mathcal{O}_K/\mathfrak{p} \,\middle|\, \mathbb{Z}/p\mathbb{Z}\right) \cong \mathrm{Gal}\left(\mathcal{O}_K/\mathfrak{p} \,\middle|\, K^{D_{\mathfrak{p}}}/\mathfrak{p}_D\right)$
canonically

and the decomposition group of $K/K^{D_{\mathfrak{p}}}$ is all
of $\mathrm{Gal}(K/K^{D_{\mathfrak{p}}})$.

Now, let $\bar{\beta}$ be a primitive elt. for $\mathcal{O}_K/\mathfrak{p}$ over $\mathcal{O}_{K^{D_{\mathfrak{p}}}}/\mathfrak{p}_D$.
Choose any lift $\beta \in \mathcal{O}_K$.
$f(x)$ = min. poly of β over $\mathcal{O}_{K^{D_{\mathfrak{p}}}}$.
Then $\bar{\beta}$ is a root of $\bar{f}(x)$, because $\bar{f}(\bar{\beta}) = \overline{f(\beta)} = \bar{0} = 0$.
Write $\bar{g}(x)$ for the min poly of $\bar{\beta}$; $\bar{g}(x) \mid \bar{f}(x)$.
The conjugates of $\bar{\beta}$ are precisely

$$\left\{\tau(\bar{\beta}) : \tau \in \mathrm{Gal}\left(\mathcal{O}_K/\mathfrak{p} \,\middle|\, \mathcal{O}_{K^{D_{\mathfrak{p}}}}/\mathfrak{p}_D\right)\right\}.$$

So each $\tau(\bar{\beta})$ is a root of $\bar{f}(x)$. Pick any τ.

There is some root $\gamma \in \mathcal{O}_K$ of $f(x)$ with $\gamma \pmod{\mathfrak{p}} = \tau(\bar{\beta})$.

Now $\mathrm{Gal}(K / K^{D_\mathfrak{p}}) = D_\mathfrak{p}$ acts transitively on the roots of f.

Choose σ with $\sigma(\beta) = \gamma$, so

$$\bar{\sigma}(\bar{\beta}) = \gamma \bmod \mathfrak{p} = \tau(\bar{\beta}).$$

Since $\bar{\beta}$ is primitive, $\bar{\sigma} = \tau$ (any auto. is determined by its action on $\bar{\beta}$).

But we're done! σ surjects onto our chosen element τ.

<u>Definition</u>. The kernel of the reduction map

$$D_\mathfrak{p} \longrightarrow \mathrm{Gal}(\mathcal{O}_K/\mathfrak{p} \mid \mathcal{O}_{K^{D_\mathfrak{p}}}/\mathfrak{p}_D)$$

(or: write $\mathrm{Gal}(k(\mathfrak{p}) \mid k(\mathfrak{p}_D))$)

is called the <u>inertia</u> group $I_\mathfrak{p}$; we have

$$I_\mathfrak{p} = \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) : \sigma(\mathfrak{p}) = \mathfrak{p} \text{ and } \sigma(x) \equiv x \bmod \mathfrak{p} \text{ for all } x \in \mathcal{O}_K\}.$$

Then $D_\mathfrak{p} / I_\mathfrak{p} \cong \mathrm{Gal}(\mathcal{O}_K/\mathfrak{p} \mid \mathbb{Z}/(p))$, a cyclic group.

We say that we have an <u>exact sequence</u>

$$0 \longrightarrow I_\mathfrak{p} \longrightarrow D_\mathfrak{p} \longrightarrow \mathrm{Gal}(\mathcal{O}_K/\mathfrak{p} \mid \mathbb{Z}/(p)) \longrightarrow 0.$$

(briefly explain)

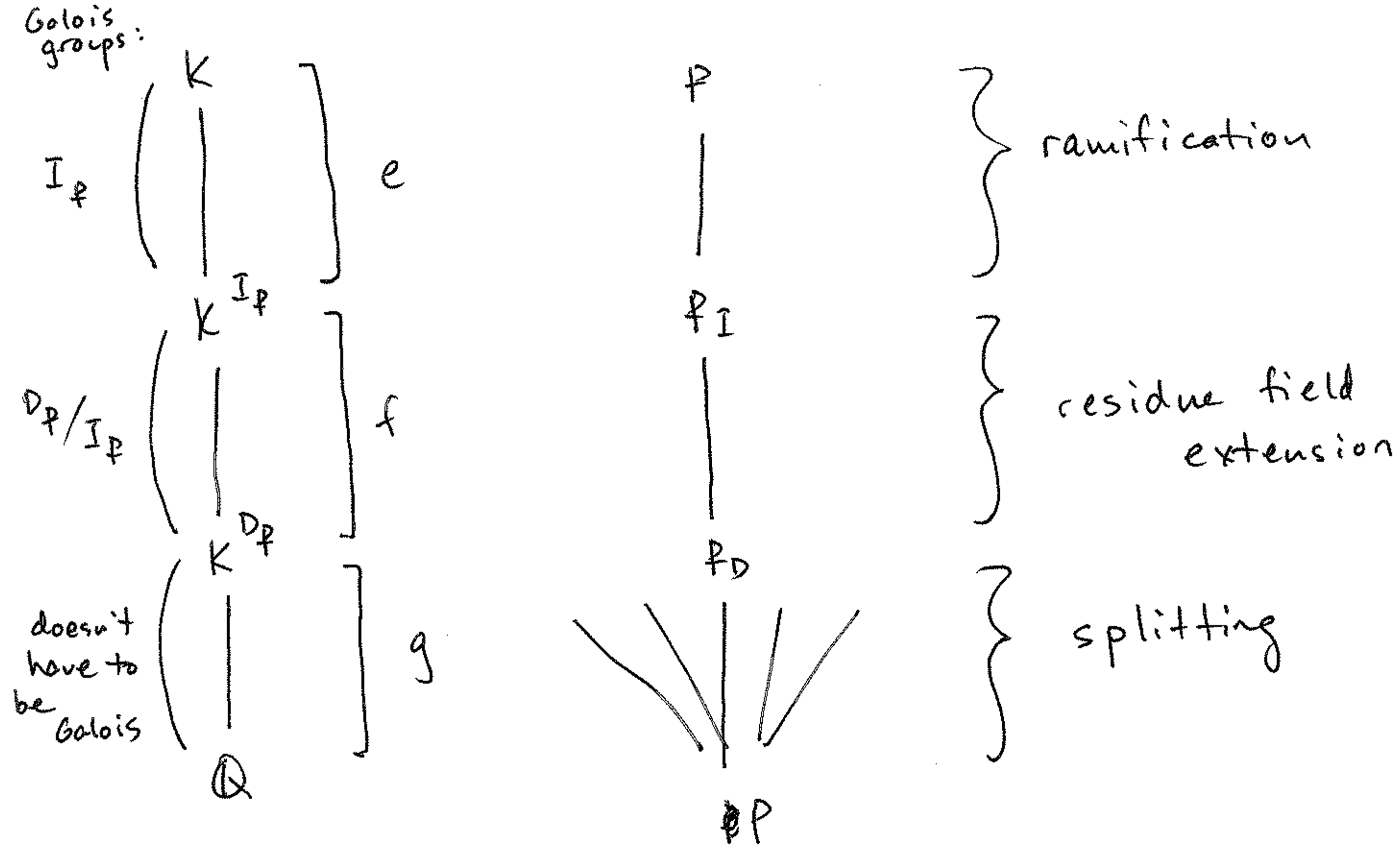
Because $|D_\mathfrak{p}| = ef$ and $|\mathrm{Gal}(\mathcal{O}_K/\mathfrak{p} \mid \mathbb{Z}/(p))| = f$,

we have $|I_\mathfrak{p}| = e$, the <u>inertia</u> group <u>measures</u> <u>ramification</u>.

$$I_\mathfrak{p} = 1 \longrightarrow \mathfrak{p} \text{ is unramified}.$$

28.4 = 29.1.

The big picture:



There is a claim here.

<u>Prop</u>. Given $\mathfrak{p}_D$ and $\mathfrak{p}$ as above, there is a unique prime $\mathfrak{p}_I$ of $K^{I_\mathfrak{p}}$ in between. We have

$e(\mathfrak{p}|\mathfrak{p}_I) = e(\mathfrak{p}|p)$ and ~~$e(\mathfrak{p}_I|\mathfrak{p}_D)$~~, $f(\mathfrak{p}|\mathfrak{p}_I) = 1$

$e(\mathfrak{p}_I|\mathfrak{p}_D) = 1$ and $f(\mathfrak{p}_I|\mathfrak{p}_D) = f(\mathfrak{p}|p)$.

<u>Proof</u>. Look at the map

$$\underbrace{\mathrm{Gal}(K/K^{I_\mathfrak{p}})}_{\text{Decomposition group of } \mathfrak{p}|\mathfrak{p}_I} \longrightarrow \mathrm{Gal}(\mathcal{O}_K/\mathfrak{p} \mid \mathcal{O}_{K^{I_\mathfrak{p}}}/\mathfrak{p}_I).$$

~~which is just the quotient~~

~~$\mathrm{Gal}(K/K^{I_\mathfrak{p}}) \hookrightarrow \mathrm{Gal}(\mathcal{O}_K/\mathfrak{p} \mid \mathcal{O}_{K^{D_\mathfrak{p}}}/\mathfrak{p}_D) \twoheadrightarrow \mathrm{Gal}(\mathcal{O}_K/\mathfrak{p} \mid \mathcal{O}_{K^{I_\mathfrak{p}}}/\mathfrak{p}_I)$~~

~~quotient by~~

It is surjective.

But, we have ~~this~~

$$\mathrm{Gal}(K/K^{I_\mathfrak{p}}) \longrightarrow \mathrm{Gal}(\mathcal{O}_K/\mathfrak{p} \mid \mathcal{O}_K{}^{I_\mathfrak{p}}/\mathfrak{p}_I) \hookrightarrow \mathrm{Gal}(\mathcal{O}_K/\mathfrak{p} \mid \mathcal{O}_K{}^{D_\mathfrak{p}}/\mathfrak{p}_D)$$

(same map)

and everything in $\mathrm{Gal}(K/K^{I_\mathfrak{p}})$ maps to 1.

Therefore, $|\mathrm{Gal}(\mathcal{O}_K/\mathfrak{p} \mid \mathcal{O}_K{}^{I_\mathfrak{p}}/\mathfrak{p}_I)| = 1 \quad (= f(\mathfrak{p} \mid \mathfrak{p}_I))$.

Recall. The extension $\mathcal{O}_K/\mathfrak{p} \mid \mathbb{Z}/(p)$ is Galois, with cyclic Galois group generated by the Frobenius automorphism

$$\phi : x \longrightarrow x^p.$$

Def. Assume $K/\mathbb{Q}$ is Galois, and $\mathfrak{p} \subseteq \mathcal{O}_K$ is unramified over p, so that the previous map is ~~is~~ an isomorphism. Then the preimage of ϕ in $D_\mathfrak{p}$ is unique, and is called the Frobenius automorphism (or Artin symbol) at $\mathfrak{p}$.

Write $(\mathfrak{p}, K/\mathbb{Q})$ or $\left(\frac{K/\mathbb{Q}}{\mathfrak{p}}\right)$.

Remarks. (if time, wax poetic)

(1) Defined for general extensions L/K (if Galois).

(2) Is this a crapshoot? Are there patterns? Relate to splitting, APs (in cyclotomic fields only)

(3) The order of $(\mathfrak{p}, K/\mathbb{Q})$ is f.
(Cor. Let $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{Sym}(3)$. No prime is totally inert!)

(4) Will associate Artin L-functions.

(5) Chebo.

(6) CFT.

29.3. Properties of the Artin symbol.

Prop. $K/\mathbb{Q}$ Galois, $G = \mathrm{Gal}(K/\mathbb{Q})$, $\tau \in G$.
Then $(\tau(\mathfrak{p}), K/\mathbb{Q}) = \tau(\mathfrak{p}, K/\mathbb{Q})\tau^{-1}$.

Proof. Check first that the both fix $\tau(\mathfrak{p})$.
LHS does by definition.
RHS: Set $\sigma = (\mathfrak{p}, K/\mathbb{Q})$,

$$\tau\sigma\tau^{-1}(\tau(\mathfrak{p})) = \tau\sigma(\mathfrak{p}) = \tau(\mathfrak{p}).$$

Now check that RHS acts as $x \to x^p \bmod \tau(\mathfrak{p})$.
If $x \in \mathcal{O}_K$,

$$\tau(\mathfrak{p}, K/\mathbb{Q})\tau^{-1}(x) = \tau\sigma\tau^{-1}(x)$$
$$= \tau\left(\tau^{-1}(x)^p + b\right) \text{ for some } b \in \mathfrak{p}$$
$$= x^p + \tau(b) \text{ for some } \tau(b) \in \tau(\mathfrak{p})$$

as desired.

Therefore. The set $\{(\tau(\mathfrak{p}), K/\mathbb{Q}) : \tau \in \mathrm{Gal}(K/\mathbb{Q})\}$ forms a conjugacy class of $\mathrm{Gal}(K/\mathbb{Q})$.
We write it $(p, K/\mathbb{Q})$. (Notation similar, but prime is downstairs.)

Frobenius in cyclotomic fields.

Let $K = \mathbb{Q}(\zeta_n)$ with $p \nmid n$ unramified.
Determine, for a prime $\mathfrak{p}$ over p, $(\mathfrak{p}, K/\mathbb{Q})$.

If $\sigma = (\mathfrak{p}, K/\mathbb{Q})$, characterized by $\sigma(x) \equiv x^p \bmod \mathfrak{p}$ for all $x \in \mathbb{Z}[\zeta_n]$.

(and $\sigma(\mathfrak{p}) = \mathfrak{p}$.)

29.4.

Claim. σ is the element $\tau := \{\zeta_n \to \zeta_n^p\}$.

Proof. For any $x = \sum a_i \zeta_n^i$, we have

$$\tau(x) = \sum a_i \zeta_n^{ip}$$
$$\equiv \sum a_i^p \zeta_n^{ip} \pmod{\mathfrak{p}} \quad (\text{since } (p) \subseteq \mathfrak{p})$$
$$\equiv \left(\sum a_i \zeta_n^i\right)^p \pmod{\mathfrak{p}}.$$

(Also shows $\tau(\mathfrak{p}) = \mathfrak{p}$.)

By uniqueness of Frobenius, τ does it! $\tau = \sigma$.

Remarks. (1) Here σ doesn't actually depend on $\mathfrak{p}$, just p. Indeed, conjugacy classes in abelian extensions are singletons.

(2) We observe that the Frobenius map induces an isomorphism

$$~~\text{Gal}~~ (\mathbb{Z}/n)^\times \xrightarrow{\sim} \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$$
$$p \longrightarrow \{\zeta_n \to \zeta_n^p\}.$$

Frobenius in quadratic fields.

Let $K = \mathbb{Q}(\sqrt{d})$, p unramified. Identify $G(K/\mathbb{Q})$ with ± 1.

Recall, the order of Frobenius is $f(\mathfrak{p}|p)$.

If $p\mathcal{O}_K$ splits, then $f(\mathfrak{p}|p) = 1$ and so $(p, K/\mathbb{Q}) = +1$.
If $p\mathcal{O}_K$ is inert, then $f(\mathfrak{p}|p) = 2$ and so $(p, K/\mathbb{Q}) = -1$.

Since $p\mathcal{O}_K$ splits iff d is a square in $\mathbb{F}_p$, $(p \neq 2)$

$$(p, K/\mathbb{Q}) = \left(\frac{d}{p}\right).$$

29.5.

Restriction of Frobenius:

Given Galois extensions L/K,

$$\begin{array}{cc} L & \mathfrak{P} \\ | & | \\ K & \mathfrak{p} \\ | & | \\ \mathbb{Q} & p \end{array}$$

p unramified in $\mathcal{O}_L$.

Then, $(\mathfrak{P}, L/\mathbb{Q})\big|_K = (\mathfrak{p}, K/\mathbb{Q})$.

Proof, "Obvious":

Write $\sigma = (\mathfrak{P}, L/\mathbb{Q})$,

for all $x \in \mathcal{O}_L$, $\sigma(x) = x^p + \beta \in \mathfrak{P}$.

If $x \in \mathcal{O}_K$ also, then β must be in $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$.

So $\sigma(x) \equiv x^p \mod \mathfrak{p}$ for $x \in \mathcal{O}_K$, QED.

Frobenius in quadratic fields another way.

Let K: ~~$\mathbb{Q}(\sqrt{p})$~~ $\mathbb{Q}(\zeta_p)$. Then $\text{Disc}(K) = \pm p^{\text{some power}}$.

By Galois theory, K contains a quadratic field.

It must be $\mathbb{Q}(\sqrt{\pm p})$ where $|\text{Disc}(\mathbb{Q}(\sqrt{\pm p}))| = p$.

So, it's $\mathbb{Q}(\sqrt{p})$ if $p \equiv 1 \mod 4$

$\mathbb{Q}(\sqrt{-p})$ if $p \equiv 3 \mod 4$.

Write $\mathbb{Q}(\sqrt{p^*})$.

The Artin symbol in K: $(q, K/\mathbb{Q}) = \{\zeta_p \to \zeta_p^q\}$.

Restrict this to $\mathbb{Q}(\sqrt{p^*})$. Is it $+1$ or -1?

Observe that $\text{Gal}(K/\mathbb{Q})$ has a unique subgroup of ~~order~~ index 2: the squares.

And $\text{Gal}(\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}) \cong \text{Gal}(K/\mathbb{Q}) / \text{Gal}(\mathbb{Q}(\sqrt{p^*})/\mathbb{Q})$. (wrong)

So $\sigma \in \text{Gal}(K/\mathbb{Q})$ reduces to $+1 \in \text{Gal}(\mathbb{Q}(\sqrt{p^*})/\mathbb{Q})$

iff σ is a square, i.e. iff $\left(\frac{q}{p}\right) = 1$.

Therefore, we have computed

$$\left(q, \mathbb{Q}(\sqrt{p^*})/\mathbb{Q}\right) = \left(\frac{q}{p}\right).$$

However, we previously computed

$$\left(q, \mathbb{Q}(\sqrt{p^*})/\mathbb{Q}\right) = \left(\frac{p^*}{q}\right).$$

Wait. what ~?

BIG THEOREM. (Gauss)

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right).$$

__Warning.__ This is the gateway drug to learn class field theory.

(... where were we ...?)

Given the following. $K/\mathbb{Q}$ Galois, $\mathfrak{p} | p$ unramified.

$D_{\mathfrak{p}} := \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) : \sigma(\mathfrak{p}) = \mathfrak{p}\}$,
the decomposition group (all of which are conjugate).

Recall $|D_{\mathfrak{p}}| = ef = f$ here, because $e = 1$,
with an isomorphism

$$D_{\mathfrak{p}} \xrightarrow{\sim} \mathrm{Gal}\left(\mathcal{O}_K/\mathfrak{p} \,/\, \mathbb{Z}/(p) \right)$$
$$\sigma \longrightarrow \sigma \text{ acts naturally.}$$

In general, set

$$1 \to I_{\mathfrak{p}} \longrightarrow D_{\mathfrak{p}} \longrightarrow \mathrm{Gal}\left(\mathcal{O}_K/\mathfrak{p} \,/\, \mathbb{Z}/(p) \right) \to 1.$$
$$I_{\mathfrak{p}} = \{\sigma : \sigma(\mathfrak{p}) = \mathfrak{p} \text{ and } \sigma(x) \equiv x \pmod{\mathfrak{p}} \text{ for all } x \in \mathcal{O}_K\}.$$

Now $\mathrm{Gal}(\mathcal{O}_K/\mathfrak{p} \,/\, \mathbb{Z}/(p))$ is generated by the Frobenius element $x \to x^p$.
Its inverse image is the Frobenius at $\mathfrak{p}$, $(\mathfrak{p}, K/\mathbb{Q})$.

Properties, proved last time.

(1) Restriction.

$$\begin{array}{cc} L & \mathfrak{P} \\ | & | \\ K & \mathfrak{p} \\ | & | \\ \mathbb{Q} & p \end{array} \qquad (\mathfrak{P}, L/\mathbb{Q})\big|_K = (\mathfrak{p}, K/\mathbb{Q}).$$

L, K Galois over $\mathbb{Q}$.

(2) Conjugation. Let $\mathfrak{p} \in \mathcal{O}_K$. We have $(\tau(\mathfrak{p}), K/\mathbb{Q}) = \tau (\mathfrak{p}, K/\mathbb{Q}) \tau^{-1}$.

So, we can write $(p, K/\mathbb{Q}) := \{(\mathfrak{p}, K/\mathbb{Q}) : \mathfrak{p} | p\}$, a conjugacy class of $G(K/\mathbb{Q})$.

30.2. Examples.

Frobenius in cyclotomic fields.

Let $K = \mathbb{Q}(\zeta_n)$ with $p \nmid n$ unramified.

Let $\mathfrak{p}$ lie over p. Find $(\mathfrak{p}, K/\mathbb{Q}) =: \sigma$.

σ is characterized by $\sigma(\mathfrak{p}) = \mathfrak{p}$ and $\sigma(x) \equiv x^p \mod \mathfrak{p}$ for all $x \in \mathbb{Z}[\zeta_n]$,

it's the unique σ so doing.

Claim. Let $\tau \in Gal(K/\mathbb{Q})$ be $\zeta_n \to \zeta_n^p$. Then $\sigma = \tau$.

Proof. If $x = \sum a_i \zeta_n^i$, we have $(a_i \in \mathbb{Z})$

$$\tau(x) = \sum a_i \zeta_n^{ip}$$
$$\equiv \sum a_i^p \zeta_n^{ip} \quad (\text{mod } \mathfrak{p}) \quad (\text{since } (p) \subseteq \mathfrak{p})$$
$$= \left(\sum a_i \zeta_n^i\right)^p \quad (\text{mod } \mathfrak{p}).$$

So $\tau(x) \equiv x^p \mod \mathfrak{p}$. (And, in particular, $\tau(\mathfrak{p}) = \mathfrak{p}$.)

So done.

Remarks.

(1) σ doesn't depend on $\mathfrak{p}$, just p.

$Gal(K/\mathbb{Q})$ is abelian, conjugacy classes are singletons.

(2) The Frobenius map induces an isomorphism

$$(\mathbb{Z}/n)^\times \longrightarrow Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$$
$$p \longrightarrow \{\zeta_n \to \zeta_n^p\}.$$

30.3.

Frobenius in quadratic fields. (1)

$K = \mathbb{Q}(\sqrt{d})$ with p UR. Identify $G(K/\mathbb{Q})$ with ± 1.

Recall, the order of Frobenius is $f(\mathfrak{p} | p)$.

So:

$p\mathcal{O}_K$ splits $\longleftrightarrow$ $f(\mathfrak{p}|p) = 1$ $\longleftrightarrow$ $(p, K/\mathbb{Q}) = 1$.

$p\mathcal{O}_K$ inert $\longleftrightarrow$ $f(\mathfrak{p}|p) = 2$ $\longleftrightarrow$ $(p, K/\mathbb{Q}) = -1$.

But recall that p splits in $\mathbb{Q}(\sqrt{d}) \longleftrightarrow \left(\frac{d}{p}\right) = 1$.

This proves, for $p \neq 2$, that

$$(p, K/\mathbb{Q}) = \left(\frac{d}{p}\right).$$

Frobenius in quadratic fields. (2).

Let $K = \mathbb{Q}(\zeta_p)$ (p odd). Then $\mathrm{Disc}(K) = \pm p^{\text{some power}}$.

By Galois theory, K contains a quadratic field.

What is it?

It *must* have discriminant $\pm p$, and therefore be $\mathbb{Q}(\sqrt{\pm p})$, in particular, $\mathbb{Q}(\sqrt{p^*})$, where

$$p^* = \begin{cases} p & \text{if } p \equiv 1 \bmod 4 \\ p & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

[Think about this! $\mathbb{Q}(\zeta_3)$ contains $\frac{1+\sqrt{-3}}{2}$, hence $\sqrt{-3}$.

But $\mathbb{Q}(\zeta_5)$ contains $\sqrt{5}$.

Inscribe a regular pentagon in a circle?

Side length $\sqrt{\frac{5-\sqrt{5}}{2}}$.

Look up regular 17-gons. related also to Gauss sums.]

30.4.

The Artin symbol in K is $(q, K/\mathbb{Q}) = \{\zeta_p \to \zeta_p^q\}$.
Restrict it to $\mathbb{Q}(\sqrt{p^*})$. Is it +1 or −1?

Recall. $\mathrm{Gal}(K/\mathbb{Q})$ has a unique subgroup of index 2.
The squares.

We have

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}) \cong \mathrm{Gal}(K/\mathbb{Q}) \big/ \mathrm{Gal}(K/\mathbb{Q}(\sqrt{p^*}))$$

$\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ reduces to $\begin{cases} 1 \in \mathrm{Gal}(\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}) \\ \quad \text{if } \sigma \text{ is a square in } \mathrm{Gal}(K/\mathbb{Q}) \\ -1 \text{ if } \sigma \text{ isn't} \end{cases}$.

If ~~σ ∈ Gal~~ $\sigma = (q, K/\mathbb{Q}) = \{\zeta_p \to \zeta_p^q\}$,
then since $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/p)^\times$
σ is a square iff q is a square mod p.

In other words, the restriction of $(q, K/\mathbb{Q})$ to
$\mathrm{Gal}(\mathbb{Q}(\sqrt{p^*})/\mathbb{Q})$ is

$$\begin{cases} +1 & \text{if } \left(\frac{q}{p}\right) = 1 \\ -1 & \text{if } \left(\frac{q}{p}\right) = -1 \end{cases}$$

That is,

$$(q, \mathbb{Q}(\sqrt{p^*})/\mathbb{Q}) = (q, K/\mathbb{Q})\Big|_{\mathbb{Q}(\sqrt{p^*})} = \left(\frac{q}{p}\right).$$

↑ restriction theorem!

But, we saw earlier that

$$(q, \mathbb{Q}(\sqrt{p^*})/\mathbb{Q}) = \left(\frac{p^*}{q}\right).$$

Were you expecting that?

BIG THEOREM. (Gauss) For all odd primes p, q,

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right).$$

This generalizes.

Cubic reciprocity: Let $\mathbb{Z}[w] = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$.

A prime π of $\mathbb{Z}[w]$ is primary if $\pi \equiv \pm 1 \pmod 3$.

(Note: Six units, and $\left|\left(\mathbb{Z}[w]/(3)\right)^*\right| = 6$. So Translate any π by a unit.)

Define a "cubic Legendre symbol" ~~leg~~ $\left(\frac{q}{\pi}\right)_3$ by

$$q^{(N(\pi)-1)/3} \equiv \left(\frac{q}{\pi}\right)_3 \mod \pi,$$

where $\left(\frac{q}{\pi}\right)_3 \in \{1, w, w^2\}$ which are all incongruent mod π.

Theorem. (Eisenstein) If π, θ are primary primes in $\mathbb{Z}[w]$ of unequal norm,

$$\left(\frac{\theta}{\pi}\right)_3 = \left(\frac{\pi}{\theta}\right)_3.$$

There is a version for ~~quar~~ biquadratic reciprocity also.

31.1. The Artin symbol and cycle types.

[Recall def. & include conjugacy class def.]

Last time. Computed,

(1) $(\mathfrak{p}, \mathbb{Q}(\zeta_n)/\mathbb{Q}) = (\zeta_n \to \zeta_n^p)$ for any $\mathfrak{p} | p$.

(2) $(\mathfrak{p}, \mathbb{Q}(\sqrt{d})/\mathbb{Q}) = \left(\frac{d}{p}\right)$ ".

~~(3) Using $\sqrt{p^*} \subseteq \mathbb{Q}(\zeta_p)$ with $p^* = \pm p$, $p^* \equiv 1 \pmod 4$,~~
~~and restriction,~~

~~$(\mathfrak{q}, \mathbb{Q}(\sqrt{p^*})/\mathbb{Q}) = \left(\frac{p^*}{q}\right)$~~

(3) Let ℓ be a prime, $\sqrt{\ell^*} \subseteq \mathbb{Q}(\zeta_\ell)$ with $\ell^* = \pm \ell$, $\ell^* \equiv 1 \ (4)$.

Use restriction, get

$(\mathfrak{p}, \mathbb{Q}(\sqrt{\ell^*})/\mathbb{Q}) = \left(\frac{p}{\ell}\right)$.

Combining (2) and (3) with $d = \ell^*$, got $\left(\frac{\ell^*}{p}\right) = \left(\frac{p}{\ell}\right)$,

Gauss's law of reciprocity.

The Chebotarev density theorem.

Def. If S is a set of primes, then the (natural) density of S is

$$\lim_{X \to \infty} \frac{\#\{p \le X : p \in S\}}{\#\{p \le X\}}$$

if the limit exists.

Thm. (Chebotarev density)
Let $K/\mathbb{Q}$ be finite and Galois with $G = G(K/\mathbb{Q})$.
Fix a conjugacy class $C \subseteq G$.
Let $S = \{p : (p, K/\mathbb{Q}) = C\}$.
Then S has density $|C|/|G|$.

Remarks.

(1) This shows that the Artin map is surjective, which is not obvious.

(2). The prime number theorem says

$$\#\{p \le x\} \sim \frac{x}{\log x},$$

so we get that too. See Lagarias + Odlyzko for an explicit error term.

(3) The proofs use L-functions!

If $\rho : \mathrm{Gal}(K/\mathbb{Q}) \to GL(V)$ is a complex representation, then

$$L(K/\mathbb{Q}, \rho, s) := \prod_{p} \det\left(1 - \left(\frac{K/\mathbb{Q}}{\mathfrak{p}}\right) p^{-s} \Big| V^{I_{\mathfrak{p}}}\right)^{-1},$$

where:

* for each p, pick any prime $\mathfrak{p}$ over p.
* The endomorphism $1 - \left(\frac{K/\mathbb{Q}}{\mathfrak{p}}\right)(N\mathfrak{p})^{-s}$ only acts on the subspace of V fixed by the inertia group $I_{\mathfrak{p}}$.

(At ramified primes there is ambiguity.)

Regard this as a technical detail, ramified primes are weird.

* It doesn't matter what $\mathfrak{p}$ you pick!

e.g. at the unramified primes,

$$1 - \left(\frac{K/\mathbb{Q}}{\mathfrak{p}}\right)(N\mathfrak{p})^{-s} \quad \text{and} \quad 1 - \left(\frac{K/\mathbb{Q}}{\mathfrak{p}'}\right)(N\mathfrak{p})^{-s} \quad \text{are}$$

conjugate endomorphisms and have the same char poly.

31.3. Example. Let $K = \mathbb{Q}(\zeta_n)$.

Then any irreducible complex ρ is of the form:

$$\rho : \mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/n)^\times \longrightarrow GL_1(\mathbb{C}) = \mathbb{C}^\times$$

$\longleftarrow$ Artin map!

i.e. it is a Dirichlet character.

So $L(K/\mathbb{Q}, \rho, s) = \prod_{p \nmid n} (1 - \rho(p) p^{-s})^{-1}$ i.e. it is just a Dirichlet L-function.

* We have

$$\zeta_K(s) = \zeta(s) \cdot \prod_{\substack{\rho \text{ irred} \\ \neq 1}} L(K/\mathbb{Q}, \rho, s)^{\dim \rho}.$$

↑ Dedekind zeta

Already interesting even in the simplest cases.

For example,

$$\zeta_{\mathbb{Q}(i)}(s) = \sum_{\underline{a} \trianglelefteq \mathbb{Z}[i]} N(\underline{a})^{-s} = \frac{1}{4} \sum_{(n,m) \neq (0,0)} (n^2 + m^2)^{-s}$$

$$= \zeta(s) \cdot L(\mathbb{Q}(i), \rho, s)$$

and $L(\mathbb{Q}(i), \rho, s) = L(s, \chi_{-4})$

$$= \sum_n \left(\frac{-1}{n}\right) \cdot n^{-s}.$$

So $$\frac{1}{4} \sum_{(n,m) \neq (0,0)} (n^2 + m^2)^{-s} = \left(\sum_n n^{-s}\right)\left(\sum_m \left(\frac{-1}{m}\right) \cdot m^{-s}\right).$$

31.4. What does Chebo say in our examples?

$\mathbb{Q}(\zeta_n)/\mathbb{Q}$. Then $(p, \mathbb{Q}(\zeta_n)/\mathbb{Q}) = \{\zeta_n \to \zeta_n^p\}$ and all these occur with equal frequency.

In other words, Chebo says that the density of $\{p : p \equiv a \pmod{n}\}$ is $\frac{1}{|(\mathbb{Z}/n)^\times|} = \frac{1}{\varphi(n)}$ for each $a \pmod{n}$ with $(a,n) = 1$.

$\mathbb{Q}(\sqrt{d})/\mathbb{Q}$. Then $(p, \mathbb{Q}(\sqrt{d})/\mathbb{Q}) = \left(\frac{d}{p}\right)$, so Chebo says, since $\left(\frac{d}{p}\right) = 1 \longleftrightarrow p$ splits in $\mathbb{Q}(\sqrt{d})$, that half of all primes split in $\mathbb{Q}(\sqrt{d})$.

Factorization with cubic polynomials.

Let $f(x) = x^3 - 2$. Factor over $\mathbb{Z}/p$ for lots of primes p.

First n primes n:	$(x-a)(x-b)(x-c)$	$(x-a)(x^2+bx+c)$	irred.
600	93	304	203
12000	1955	6022	4027

$f(x) = x^3 - 7x + 7$:

600	199	0	401
12000	4002	0	7998.

31.5.) → 32.3.

We compute the Galois groups: (of the splitting fields)

What is $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$? Let $K = \mathbb{Q}(\sqrt[3]{2})$

Let σ: $\sqrt[3]{2} \to \zeta_3 \cdot \sqrt[3]{2}$. So $\sigma \in K$, $\sigma^3 = 1$.

K contains ζ_3 and so $\sqrt{-3}$. $\tau: \sqrt{-3} \to -\sqrt{-3}$.

$\zeta_3 \to \zeta_3^2$.

$\tau \in K$, $\tau^2 = 1$.

Note $\sigma\tau(\sqrt[3]{2}) = \sigma(\sqrt[3]{2}) = \zeta_3 \cdot \sqrt[3]{2}$

$\tau\sigma(\sqrt[3]{2}) = \tau(\zeta_3 \cdot \sqrt[3]{2}) = \zeta_3^2 \cdot \sqrt[3]{2}$.

So $\sigma\tau = \tau^2\sigma$, $\mathrm{Gal}(K/\mathbb{Q}) = S_3$.

What about $x^3 - 7x + 7$? Discriminant is 49 (a square).

This implies the Galois group is C_3. Why?

Let $x^3 - 7x + 7 = (x-\theta_1)(x-\theta_2)(x-\theta_3)$.

Then $\mathrm{Disc}(\mathbb{Z}[\theta_i]/\mathbb{Z}) = 49 \cdot n^2 = [(\theta_1-\theta_2)(\theta_2-\theta_3)(\theta_3-\theta_1)]^2$

so $a := (\theta_1-\theta_2)(\theta_2-\theta_3)(\theta_3-\theta_1) \in \mathbb{Q}$.

Let $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ and suppose (WLOG) $\sigma(\theta_1) = \theta_2$.

What is $\sigma(\theta_2)$? If it's θ_1, apply σ to above:

$\sigma(a) = (\theta_2-\theta_1)(\theta_1-\theta_3)(\theta_3-\theta_2) = -a$.

But $\sigma(a) = a$. Therefore we must have $\sigma(\theta_2) = \theta_3$.

So the Galois group is C_3.

To explain this phenomeon:

(1) Understand relation btn. Galois and the roots.

(2) Understand relation to the Frobenius element.

(1). **Theorem.** (Milne, 8.21)

Let $f(x)$ monic deg. n over K. (Maybe not irred.)

G = Galois group of $f(x)$ (i.e. of L/K, where L is the splitting field)

Then G acts on the roots of $f(x)$. Suppose it has s orbits with $n_1, \dots, n_s$ elements $(n_1 + \dots + n_s = n)$.

Then,

$$f(x) = f_1(x) \cdots f_r(X) \quad \text{in } K,$$

with the f's irreducible.

Proof. This is Galois theory.

Write $f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$.

For any subset $S \subseteq \{\alpha_1, \dots, \alpha_n\}$ of the roots, let

$$f_S := \prod_{\alpha_i \in S} (X - \alpha_i).$$

Then, f_S has coefficients in K

$$\Updownarrow$$

$\mathrm{Gal}(L/K)$ fixes f_S

$$\Updownarrow$$

$\mathrm{Gal}(L/K)$ permutes the α_i.

So the minimally permuted sets (i.e. the orbits) correspond precisely to the irreducible factors.

Corollary. Let $f(x)$ be monic separable over a finite field k,

$\lambda :=$ splitting field.

Suppose the Frobenius elt $\sigma \in Gal(\lambda / k)$ acts as a product of an n_1 cycle, an n_2 cycle, ... a n_s-cycle (with $n_1 + \cdots + n_s = n$) on the roots of f.

Then $f(x) = f_1(x) \cdots f_r(x)$ in k.

So we get what we want:

Theorem. (Dedekind) Let $f(x)$ monic, irred over O_K for a NF K,

$G =$ Galois group of f.

Suppose $\mathfrak{p}$ is a prime ideal of K with

$f(x) \equiv f_1(X) \cdots f_r(X) \mod \mathfrak{p}$, with

$f_1, \ldots f_r$ irreducible and distinct polynomials of degree n_i in $(O_K/\mathfrak{p})[x]$.

~~Then the Frobenius element~~

If $\mathfrak{P}$ is any prime of the splitting field L of f over $\mathfrak{p}$, then $(\mathfrak{P}, L/K)$ acts as a product of r cycles of length n_i.

Proof. Notice that ~~the~~ $\mathfrak{p}$ is unramified in L/K, because $\mathfrak{p}$ doesn't divide the discriminant of f.

In particular, all of the roots of $f(x)$ are distinct mod $\mathfrak{P}$.

So $(\mathfrak{P}, L/K)$ acts as Frobenius on $\lambda | k$.

Use the corollary.

32.5.

Let L be the splitting field of $x^3 - 2$.

Any $\sigma \in \text{Gal}(L/\mathbb{Q})$ acts by permuting the roots.
(Reorder the roots – conjugate σ.)

$x^3 - 2 = (x-a)(x-b)(x-c) \mod p \longleftrightarrow (p, L/\mathbb{Q})$ is 3 1-cycles. the trivial elt. of S_3.

$= (x-a)(x^2+bx+c) \longleftrightarrow (p, L/\mathbb{Q})$ has cycle type $(1)(2)$. (3 elts.)

$=$ irred. $\longleftrightarrow (p, L/\mathbb{Q})$ is a 3-cycle.

These occur in $\text{Gal}(L/\mathbb{Q})$ with freq. $1:3:2$.
Chebo $\Rightarrow$ same frequency for the primes.

$x^3 - 7x + 7 = (x-a)(x-b)(x-c) \mod p \longleftrightarrow$ 3 1-cycles

$(x-a)(x^2+bx+c) \mod p \longleftrightarrow (p, L/\mathbb{Q})$ has cycle type $(1)(2)$

irred. $\longleftrightarrow$ 3-cycle.

But the Galois group is C_3, and only the first two cycle types occur.

32.6.

Example. Determine $Gal(L/\mathbb{Q})$, where L is the splitting field of $f(x) = x^4 - 4x + 2$.

Sol'n. Factor mod some primes.

$p = 2 \to$ repeated root (2 ramifies. ignore.)

$p = 3 \to$ irred.

$p = 5 \to$ (monic) · (cubic)

$p = 7$ "

$p = 13 \to$ (monic) (monic) (quadratic)

⋮

What is this telling us?

$Gal(K/\mathbb{Q}) \subseteq S_4$ contains a 4-cycle, say $(1\ 2\ 3\ 4)$.

Also contains a 2-cycle. If $(1\ 2)$, $(2\ 3)$, $(3\ 4)$, $(4\ 1)$ then ~~done~~ get S_4.

But it might be $(1\ 3)$ or $(2\ 4)$.

Then we get at least D_4.

But we also contain an elt. of order 3! So all of A_4.

Ex. $f(x) = x^4 + 3x^2 + 7x + 4$.

Prove Galois is A_4.

Ex. $f(x) = x^4 - 2x^2 - 11$.

Galois is D_4. (That's hard.)

Can guess by Chebo/proportions.

But you can always prove S_n in this way!

33.1. Definition. Let K be a number field. Then the maximal unramified abelian extension of K is called the Hilbert class field of K.

[Implicit: If L, L' are UR abelian / K, so is $L \cdot L'$.]

[Ramification includes at infinity: real places stay real.]

Examples. * $K = \mathbb{Q}$. is its own HCF.

* $K = \mathbb{Q}(\sqrt{-14})$. Then the HCF is $L = K(\alpha)$, with $\alpha = \sqrt{2\sqrt{2}-1}$. $[L : K] = 4$.

Let $K = \mathbb{Q}(\sqrt{-D})$ with integral basis $[1, \tau]$.

So $\tau = \sqrt{-D}$ or $\frac{1+\sqrt{-D}}{2}$

Define
$$g_2(\tau) = 60 \sum_{(m,n)\neq(0,0)} (m+n\tau)^{-4}$$
$$g_3(\tau) = 140 \sum_{(m,n)\neq(0,0)} (m+n\tau)^{-6}$$
$$j(\tau) = 1728 \cdot \frac{g_2(\tau)^3}{g_2(\tau)^3 - 27 g_3(\tau)^2}.$$

Then $K(j(\tau))$ is the Hilbert class field of K.
(See Cox, Ch. 11 or ask Matt)
(Related fact: compute $e^{\pi\sqrt{163}}$.)

We defined the Artin map
$$\left(\frac{H/K}{\cdot}\right) : I_K \longrightarrow \mathrm{Gal}(H/K).$$
(I_K: ideals (fractional) on K.)

Defined it for all primes, and just extend by multiplicativity.

Theorem. The Artin map is surjective, and its kernel is exactly the subgroup of principal ideals P_K. Therefore, $\left(\frac{L/K}{\cdot}\right)$ induces an isomorphism
$$Cl(K) \xrightarrow{\sim} \mathrm{Gal}(H/K).$$

 We want to say, e.g.

$$(\mathbb{Z}/n)^\times \to \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \text{ is an example.}$$

But,
$(\mathbb{Z}/n)^\times$ is not the class group of $\mathbb{Q}$, and
$\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is not unramified.

So we define ray class groups.
If K is a number field, define a modulus of K to be a "formal ideal" $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_\mathfrak{p}}$

with: $n_\mathfrak{p} \geq 0$, and at most finitely many are nonzero
Real primes $\mathfrak{p}$ (i.e. embeddings $K \hookrightarrow \mathbb{R}$) are allowed with $n_\mathfrak{p} = 0$ or 1.
(Snobby highbrow view: "primes" = "places" = "valuations"!)

So any modulus $\mathfrak{m}$ may be written $\mathfrak{m} = \mathfrak{m}_0 \mathfrak{m}_\infty$
$\mathfrak{m}_0$: an $\mathcal{O}_K$-ideal
$\mathfrak{m}_\infty$: formal product of distinct real inf. primes of K.

Given $\mathfrak{m}$, define:

$I_K(\mathfrak{m})$ = all fractional ideals coprime to $\mathfrak{m}$ (which means coprime to $\mathfrak{m}_0$)

$P_K(\mathfrak{m})$ = all principal ideals $\alpha\mathcal{O}_K$, where:

$\alpha \equiv 1 \pmod{\mathfrak{m}}$,
$\sigma(\alpha) > 0$ for every real infinite prime dividing $\mathfrak{m}_\infty$
(if this is true for all σ: call it "totally positive")

$$Cl_\mathfrak{m}(K) := I_K(\mathfrak{m}) / P_K(\mathfrak{m}).$$

33.3.

Theorem. (Beefed up Artin reciprocity) ("existence theorem").

Given K and a modulus $\mathfrak{m}$. Then there exists a unique abelian extension L, such that $\left(\frac{L/K}{\mathfrak{p}}\right)$ induces an ~~iso~~homomorphism

$$I_K(\mathfrak{m}) \longrightarrow \mathrm{Gal}(L/K)$$

whose kernel is exactly $P_K(\mathfrak{m})$, i.e. an isomorphism

$$Cl_K(\mathfrak{m}) \xrightarrow{\sim} \mathrm{Gal}(L/K).$$

Moreover, L/K is ramified only at primes dividing $\mathfrak{m}$.

Is this what we want? Suppose $K = \mathbb{Q}$, $\mathfrak{m} = (n)$.

Is $Cl_K(\mathfrak{m}) = (\mathbb{Z}/n)^\times$?

$$Cl_K(\mathfrak{m}) = I_K(\mathfrak{m}) / P_K(\mathfrak{m}),$$

$$I_K(\mathfrak{m}) = \{(a) : a \text{ coprime to } n\}.$$

$$P_K(\mathfrak{m}) = \{(a) : a \equiv 1 \pmod{n}\}.$$

But wait: $a \equiv -1 \pmod{n}$ is okay too, because $(a) = (-a)$.

Also, have to worry about fractional ideals.

So set $\mathfrak{m} = (n)\infty$ and let's do this again.

33.4.

$I_{\mathbb{Q}}(\mathfrak{m}) = \{ (\frac{a}{b})$ coprime to n, i.e. in lowest terms a, b coprime to $n \}$.

Think of it as the group generated by $a \in \mathbb{Z}$ coprime to n
(with group operation = multiplication).

$P_{\mathbb{Q}}(\mathfrak{m}) = \{ (\frac{a}{b}) : \frac{a}{b} \equiv 1 \bmod n$, and $\frac{a}{b} > 0 \}$.

We see the infinite place again!

What does $\frac{a}{b} \equiv 1 \pmod{n}$ mean?
It could mean two things:

(1) $a \equiv b \pmod{n}$, or
(2) $a \equiv b \equiv 1 \pmod{n}$ (in analogy to above).

But these are the same, because if $a \equiv b \equiv r \pmod{n}$ with $r \cdot \bar{r} \equiv 1 \ (n)$,

then $\frac{a}{b} = \frac{a\bar{r}}{b\bar{r}}$ and $a\bar{r} \equiv b\bar{r} \equiv 1 \pmod{n}$.

What is $\{ (\frac{a}{b})$ coprime to $n \} / \{ (\frac{a}{b}), \frac{a}{b} \equiv 1 \ (n), > 0 \}$?

(1) Given $\frac{a}{b}$, multiply by $b \cdot \bar{b}$, where $b \cdot \bar{b} \equiv 1 \pmod{n}$.
So represent anything by an integer.

~~Claim: If $r \equiv s \pmod{n}$ then~~

(2) If $r \equiv s \pmod{n}$ then r and s are the same in this group.
So represent anything by an integer mod n.

(3) If $r \not\equiv s \pmod{n}$ then r and s are not the same in this group (not in the denominator group)

So $Cl_{\mathbb{Q}}(n \cdot \infty) = (\mathbb{Z}/n)^\times$.

<u>33.5</u>. This is what we want.

$$(\mathbb{Z}/n)^\times = Cl_{\mathbb{Q}}(n \cdot \infty) \xrightarrow{\sim} Gal(K/\mathbb{Q})$$
$$p \longrightarrow \left(\frac{K/\mathbb{Q}}{p}\right)$$

and K is <u>abelian</u>, ramified only at p.
It turns out that K is indeed $\mathbb{Q}(\zeta_p)$.