22.1. Dirichlet's Unit Theorem.

Let K be a NF, $\mathcal{O}_K^\times$ = group of units.
Write $\deg K = n = r + 2s$ as usual.
Let $\mu(K) \subseteq \mathcal{O}_K^\times$ be the roots of unity.
(Note: If they are in K they are in $\mathcal{O}_K$).

Theorem. $\mathcal{O}_K^\times \cong \mathbb{Z}^{r+s-1} \times \mu(K)$ as abelian groups.

~~Example: Real quadratic fields, K = Q, s ∈ ...~~

So, there is a fundamental system of units $u_1 \cdots u_{r+s-1}$ so that every unit of $\mathcal{O}_K$ can be written uniquely as

$$u = u_1 \cdots u_{r+s-1} \cdot \underbrace{\zeta_m^a}_{\text{mth root of unity to the ath power}}.$$

Examples.

$K = \mathbb{Q}$. $(r = 1, s = 0)$ $\mathbb{Z}^\times = \{\pm 1\}$.

$K = \mathbb{Q}(\sqrt{-D})$ $(r = 0, s = 1)$ $\mathcal{O}_K^\times$ = roots of unity.

(will see: $D = -3$: $|\mathcal{O}_K^\times| = 6$
$D = -4$: $|\mathcal{O}_K^\times| = 4$
else $|\mathcal{O}_K^\times| = 2$.)

$K = \mathbb{Q}(\sqrt{+D})$ $(r = 2, s = 0)$.

There is a fundamental unit ε,

$$\mathcal{O}_K^\times = \langle \varepsilon \rangle \times \pm 1 = \varepsilon^{\mathbb{Z}} \times \pm 1.$$

(why no other roots of unity ?)

So there is a unique fundamental unit ε with $\varepsilon > 1$.

(Multiply by ± 1, replace ε with $\frac{1}{\varepsilon}$)

22.2. Find them by means of Pell's equation $x^2 - dy^2 = \pm 1$ or ± 4

continued fractions.

$\mathbb{Q}(\sqrt{2})$: $1+\sqrt{2}$.
$\mathbb{Q}(\sqrt{3})$: $2+\sqrt{3}$.
$\mathbb{Q}(\sqrt{31})$: $1520 + 273\sqrt{31}$.
$\mathbb{Q}(\sqrt{94})$: (a mess)

K : a cubic field. Then $r+s-1 = 1$ or 2.
Also not many roots of unity.
(Ex. A cubic field cannot contain a primitive mth root of unity unless $m = 1, 2, 3$, or 6.)

The basic proposition.

Let $\alpha \in \mathcal{O}_K$. Then,

α is a unit $\longleftrightarrow$ $N(\alpha) = \pm 1$.

Proof. $\longrightarrow$ If $\alpha \cdot \alpha^{-1} = 1$ in $\mathcal{O}_K$, then $N(\alpha) \in \mathbb{Z}$
$N(\alpha^{-1}) \in \mathbb{Z}$
But $N(\alpha^{-1}) = \dfrac{1}{N(\alpha)}$.

$\longleftarrow$. Let α_i be the conjugates. Then,
$\alpha \cdot (\prod \alpha_i) = \pm 1$.
The α_i aren't necessarily in $\mathcal{O}_K$, but $\prod \alpha_i = \pm \dfrac{1}{\alpha} \in K$
and the α_i are algebraic integers (in $\mathcal{O}_{\bar{K}}$)
so $\prod \alpha_i \in \mathcal{O}_K$.

Caution. Must assume $\alpha \in \mathcal{O}_K$.
For example, let $\alpha = \dfrac{2+i}{2-i} \in \mathbb{Q}(i)$.
Then $N(\alpha) = \dfrac{2+i}{2-i} \cdot \dfrac{2-i}{2+i} = 1$.
But $\alpha \notin \mathcal{O}_K$ so we don't say it's a unit.
(Recall: 5 splits in $\mathbb{Q}(i)$, $(5) = (2+i)(2-i)$.

22.3. Example of how to work with units.

Let $K = \mathbb{Q}(\sqrt{-d})$

$\mathcal{O}_K = \mathbb{Z}[\sqrt{-d}]$ (so $-d \equiv 2, 3 \pmod 4$).

Then $N(a + b\sqrt{-d}) = a^2 + db^2$.

This is ± 1 only for:

$a = \pm 1$, $b = 0$.

$d = 1$, $b = \pm 1$, $a = 0$.

($\pm i$: fourth roots of unity)

So we found all the units in such fields.

Exercise. Do this for $K = \mathbb{Q}(\sqrt{-d})$, $-d \equiv 1 \pmod 4$, and $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right]$.

Example. Let $[K:\mathbb{Q}] = 3$ and $r = s = 1$.

Then, $\varepsilon^3 > \frac{1}{4}(|\Delta_K| - 24)$.

How is this useful? Let $K = \mathbb{Q}(\alpha)$ where $\alpha^3 + 10\alpha + 1$.

The discriminant is -4027.

So $\varepsilon^3 > \sqrt[3]{\frac{4027-24}{4}} > 10$.

Note that α is a unit, because $N_{K/\mathbb{Q}}(\alpha) = -1$.

Conjugates multiply to -1).

$\alpha \approx -0.099\ldots$ (Newton's method)

$-\frac{1}{\alpha} = 10.00998\ldots$ must be the fundamental unit.

22.4. The big picture.

These often turn up.

Let K be a real quadratic field. $K = \mathbb{Q}(\sqrt{d})$.

Then Dirichlet's class number formula says,

$$L(1, \chi_d) = \sum_n \left(\frac{d}{n}\right) \cdot \frac{1}{n} = \frac{h(d) \cdot \log(\varepsilon)}{\sqrt{d}}.$$

And, more generally,

$$\lim_{s \to 1^+} (s-1) \underbrace{\zeta_K(s)}_{\substack{\text{The Dedekind zeta} \\ \text{function } \sum_{\underline{a}} (N\underline{a})^{-s}}} = \frac{2^r (2\pi)^s \cdot R_K \cdot h_K}{\# \mu(K) \cdot |\Delta_K|^{1/2}},$$

where R_K is the regulator (we'll see it later)

Prototype for the Birch and Swinnerton-Dyer conjecture

regulator! (determinant involving $E(\mathbb{Q})$)

real period.

Tamagawa number

$$\underbrace{L(E,1)}_{\substack{\text{only recently} \\ \text{known to be} \\ \text{defined}}} \sim (s-1)^r \cdot \frac{R_E \cdot \Omega_E \cdot \prod_{p|N} c_p \cdot |Ш(E)|}{(\# \operatorname{Tor}(E))^2}$$

rank of E:

$E(\mathbb{Q}) \cong \mathbb{Z}^r \times \operatorname{Tor}(E)$.

(look familiar??)

Tate-Shafarevich group. believed to be finite. (Failure of local-global!) Like h_K.

(22.5) = 23.1. How are we going to prove it?

Use the geometry of numbers again. (1843 Easter Mass, Sistine Chapel)

Before, used

$K \xrightarrow{\sigma} \mathbb{R}^r \times \mathbb{C}^s$

$a \longrightarrow (\sigma_1(a), \ldots, \sigma_r(a), \underbrace{\sigma_{r+1}(a), \ldots \sigma_{r+s}(a)}_{\text{one from each pair}})$

Proved $\mathrm{Im}(K)$ is a <u>full</u> <u>lattice</u>.

This time:

$K^* \xrightarrow{\psi} \mathbb{R}^{r+s}$

$a \longrightarrow (\log|\sigma_1(a)|, \ldots, \log|\sigma_r(a)|, 2\log|\sigma_{r+1}(a)|, \ldots 2\log|\sigma_{r+s}(a)|)$.

Then $\log(|N_{K/\mathbb{Q}}(a)|) =$ sum of coeffs.
(Interested: when is it zero?)

The <u>plan</u>.

(1) Show $\psi(\mathcal{O}_K^\times)$ is a <u>lattice</u> in $\mathbb{R}^{r+s}$
and $\mathrm{Ker}(\psi)$ is finite.

Proves, the free abelian part has rank $\leq r+s$.
(And, indeed, we cut it down by one dimension: want sum $= 0$)

(2) Show $\mathrm{rk}(\psi(\mathcal{O}_K^\times)) = r+s-1$.
Use our previous construction to cook up units.

Lemma on lattices (proof omitted) (but see 18.1).

Let V be a f.d. vector space, $\Gamma \subseteq V$ a subgroup. TFAE:

(1) Γ is a lattice (e.g. a basis for Γ is l.i. over $\mathbb{R}$)

(2) Γ is discrete (i.e. given $\gamma \in \Gamma$, $\exists$ U open, $U \cap \Gamma = \{\gamma\}$)

(3) For any bounded set $B \subseteq V$, $B \cap \Gamma$ is finite.

Proposition. $\psi(\mathcal{O}_K^\times)$ is a lattice in $\mathbb{R}^{r+s}$.

Indeed, in $\{x = (x_1, \cdots, x_{r+s}) : \sum x_i = 0\}$

which is a subspace of dimension $r+s-1$.

Therefore, $\operatorname{rk}(\mathcal{O}_K^\times) \le r+s-1$.

Proof. Verify (3).

Given a bounded set B.

WLOG, $B = \{(x_1, \cdots, x_{r+s}) \in V : |x_i| \le M\}$.

(If B is not such a set, $B \subseteq B'$ where B' is.

$B' \cap \Gamma$ finite $\Rightarrow B \cap \Gamma$ finite.)

Suppose $\underset{\psi(u)}{\overset{\gamma}{\shortparallel}} \in B \cap \psi(\mathcal{O}_K^\times)$. Then, $|\sigma_j(u)| \le e^M$ for all j.

Look at $f(x) = \prod (x - \sigma_j(u))$.

Then the degree is $[K:\mathbb{Q}]$, fixed,

the coefficients are bounded,

so only finitely many possibilities for $f(x)$!

Hence for u.

Corollaries.

(1) $\operatorname{Ker} \psi : U \to \mathbb{R}^{r+s}$ is finite.

~~It is contained with~~ (Image is contained within any B containing 0.)

(2) $\operatorname{Ker} \psi \subseteq \mu(K)$.

Proof. $\operatorname{Ker}\psi$ is a finite subgroup of $\mathcal{O}_K^\times$,

hence if $u \in \operatorname{Ker}\psi$, $u^m = 1$ for some m.

23.3.

Lemma 1. Fix m with $1 \le m \le r+s$.

For all $\alpha \in \mathcal{O}_K$, there exists $\beta \in \mathcal{O}_K$ s.t.

(1) $|N_{K/\mathbb{Q}}(\beta)|$ is bounded (call the bound M)

(2) If $\psi(\alpha) = (a_1, \cdots, a_{r+s})$

$\psi(\beta) = (b_1, \cdots, b_{r+s})$

then $b_i < a_i$ except for $i = m$.

In fact we can take $M = \left(\frac{2}{\pi}\right)^s |\Delta_K|^{1/2}$.

(Will use to produce units!)

Proof. Use Minkowski's lattice point theorem.

Use the "additive mapping"

$\sigma : K \hookrightarrow \mathbb{R}^{r+2s}$

$\alpha \longrightarrow (\sigma_1(\alpha), \cdots, \sigma_r(\alpha), \operatorname{Re}\sigma_{r+1}(\alpha), \operatorname{Im}\sigma_{r+1}(\alpha), \cdots)$

Proved previously, $\sigma(\mathcal{O}_K)$ is a lattice of volume $2^{-s}|\Delta_K|^{1/2}$

Minkowski $\Rightarrow$ any big enough convex body contains lattice pts.

Define a box $E \subseteq \mathbb{R}^{r+2s}$ $\quad E = \{(x_1, \cdots, x_{r+2s}) :$

$|x_i| < e^{a_i}$ for real embeddings

$x_{r+1}^2 + x_{r+2}^2 < e^{a_{r+1}}$

$\vdots$

$x_{2r-1}^2 + x_{2r}^2 < e^{a_{r+s}}$

except for m. For m, ask that

$|x_m|$ or $x_{j+1}^2 + x_{j+2}^2 < c$, defined

s.t. $\displaystyle\prod_{i \ne m} e^{a_i} \cdot c > \left(\frac{2}{\pi}\right)^s |\Delta_K|^{1/2}$.

Then, $\operatorname{Vol}(E) = 2^r \cdot \pi^s \cdot \left(\prod_{i \ne m} e^{a_i} \cdot c\right) > 2^{r+s} |\Delta_K|^{1/2}$

$= 2^{r+2s} \operatorname{Vol}(\sigma(\mathcal{O}_K))$

and so E must contain a nonzero lattice point.

By construction it must satisfy (1) and (2), q.e.d.

25.4.

Proposition. ("unit factory")

Again fix m, $1 \le m \le r+s$.

There exists $u \in \mathcal{O}_K^\times$ s.t. if $\varphi(u) = (y_1, \cdots, y_{r+s})$,

then for each $i \ne m$ we have $y_i < 0$.

(Will show: $r+s-1$ of these will be linearly independent.)

(Remark: when $r+s=1$ this is not interesting.)

Proof. Start with any $\alpha_1 \in \mathcal{O}_K \setminus 0$.

By the lemma, choose a sequence of elements $\alpha_i \in \mathcal{O}_K$ such that

$$\begin{array}{llllll}
\alpha_1 \xrightarrow{\varphi} & (a_{1,1}, & \cdots & a_{1,m} & \cdots & a_{1,r+s}) \\
 & \quad \vee & & \text{- no guarantee} & & \quad \vee \\
\alpha_2 \xrightarrow{\varphi} & (a_{2,1} & \cdots & a_{2,m} & & a_{2,r+s}) \\
 & \quad \vee & & & & \quad \vee \\
\alpha_3 \xrightarrow{\varphi} & (a_{3,1} & \cdots & a_{3,m} & \cdots & a_{3,r+s}) \\
\vdots & & & & &
\end{array}$$

Now the α_i all generate principal ideals.

By the lemma, except for α_1 they all have norm $\le M = \left(\frac{2}{\pi}\right)^s |\Delta_K|^{1/2}$.

Only finitely many ideals of bounded norm

So some α_j and α_k generate the same ideal and hence differ by a unit. $(k > j)$

By construction, if $\alpha_k = u \cdot \alpha_j$, then

$$\varphi(\alpha_k) = \varphi(u) + \varphi(\alpha_j)$$

and u has the desired entries. QED.

Note. We will have $y_m > 0$ because $\sum y_i = 0$.

23.5.

Choose $u_1, \cdots, u_{r+s}$ according to proposition, with $\psi(u_m) > 0$, all other $\psi(u_i) < 0$.

(i.e. $|\sigma_m(u_m)| > 1$ and $|\sigma_i(u_m)| < 1$.)

Define an $(r+s) \times (r+s)$ matrix $A := \begin{pmatrix} \psi(u_1) \\ \vdots \\ \psi(u_{r+s}) \end{pmatrix}$.

Want to show. $r+s-1$ of them are independent.

Boring linear algebra lemma.

Let $B = (b_{ij})$ be a $k \times k$ real matrix.

Suppose $b_{ii} > 0$, $b_{ij} < 0$ for $j \neq i$, $\sum_j b_{ij} = 0$ for each i.

Then $\operatorname{rank}(B) = k-1$.

(and this does it)

Proof. Note the columns all live in a dim $k-1$ subspace.

Show first $k-1$ columns are independent.

Suppose $c_1 \vec{v_1} + \cdots + c_{k-1} \vec{v_{k-1}} = 0$ (v_i : ith column.)

Without loss of generality, $|c_1|$ is the largest of the $|c_i|$ (by reordering)

$c_1 = 1$ (divide through by c_1)

Look at the first row:

$$\underbrace{c_1}_{=1} \underbrace{b_{11}}_{\text{positive}} + c_2 \underbrace{b_{12}}_{\text{neg.}} + \cdots + c_{k-1} \underbrace{b_{1(k-1)}}_{\text{neg.}} = 0.$$

So ~~ege~~ $b_{11} + b_{12} + \cdots + b_{1(k-1)} \leq 0$

Now $b_{1k} < 0$, so

$b_{11} + b_{12} + \cdots + b_{1k} < 0$ but it equals zero, contradiction.

23.3.) - 2011

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

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.

The decomposition of primes.

Theorem. 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 $p^{f(p)} \equiv 1 \pmod{m}$.
(index of p mod m)
(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 $f(p)$.

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

(25.4) = 26.2

Some interesting numerical data.

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

primitive roots.

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

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

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

$p \equiv 2, 4 \pmod 7$: $p = \mathfrak{p}_1 \mathfrak{p}_2$ 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 $(\mathbb{Z}/5)^\times$. $f(\mathfrak{p}|2) = 4$.

$5\mathcal{O}_K = (\mathfrak{p}_1 \mathfrak{p}_2)^4$ $f(\mathfrak{p}_i | 5) = 1$ 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 $p^k \equiv 1 \bmod n$, then $\zeta_n^{p^k} = \zeta_n$.

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

(25.5) If $\tau^k = id$, then $\zeta_n^{p^k} - \zeta_n \in \mathfrak{p}$.
$\Downarrow$
26.3. 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 mod $\mathfrak{p}$
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
$$Gal\left(\mathbb{Z}[\zeta_n]/\mathfrak{p} \mid \mathbb{Z}/(p)\right),$$
it is the Frobenius map $\{a \longrightarrow a^p\}$.

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

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

26.4.

The ramified case.

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

We have

$$\begin{tikzcd}[column sep=small]
 & & \mathbb{Q}(\zeta_n) \arrow[dl, dash] \arrow[dr, dash] & & \\
\mathfrak{p}^{\varphi(p^r)} \arrow[ddrr, dash] & \mathbb{Q}(\zeta_{p^r}) \arrow[dr, dash] & & \mathbb{Q}(\zeta_m) \arrow[dl, dash] & \mathfrak{p}_1 \cdots \mathfrak{p}_s, \text{ where } f(\mathfrak{p}_i \mid p) = f(p). \arrow[ddll, dash] \\
 & & \mathbb{Q} & & \\
 & & p & &
\end{tikzcd}$$

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

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

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

But this takes up all the room!

Since $\sum_{i=1}^{s} \varphi(p^r) \cdot f(p) = \varphi(p^r) \cdot f(p) \dfrac{\varphi(m)}{f(p)} = \varphi(p^r)\varphi(m)$

$= \varphi(n)$,

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.

26.5.

Lamé and Kummer, on Fermat's Last Theorem.

<u>Fermat's last theorem</u>. 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.
<u>Theorem</u>. (Kummer) If $p \nmid h(\mathbb{Q}(\zeta_p))$, then FLT is true for exponent p.

Will prove: "First case of FLT":

<u>Thm.</u> 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 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 $q \mid \mathfrak{p} \cdot y$.

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

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

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

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 $p \nmid h(\mathbb{Q}(\zeta_p))$ ~~so~~ 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 $\alpha = a_0 + a_1 \zeta_p + a_2 \zeta_p^2 + \dots + a_{p-2} \zeta_p^{p-2}$

By the "Freshman Binomial Theorem",

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

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

Lemma. Let $\alpha = a_0 + a_1 \zeta_p + a_2 \zeta_p^2 + \dots + a_{p-1}\zeta_p^{p-1}$ 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 $1 + \zeta_p + \dots + \zeta_p^{p-1} = 0$.

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.

($\longrightarrow$)

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

Take $i=1$, write $q = a_1$. $x + \zeta_p y = u q^p$ for some unit.

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

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

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

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

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 $p \mid x$.

27.3. (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: $x \equiv 1 \pmod{\sigma(\mathfrak{p})}$

$$\Downarrow$$

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

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

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 $\sigma \in Gal(K/\mathbb{Q})$,

$$\begin{aligned} \sigma : \quad & K \to K \\ & \mathcal{O}_K \to \mathcal{O}_K \\ & \mathfrak{p} \to \mathfrak{p}' \end{aligned}$$

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

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

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.

$$\begin{array}{ll} K & \\ \Big| & \Big]\, ef \\ K^{D_\mathfrak{p}} & \\ \diagdown\ \big|\ \big|\ \diagup & \Big]\, g \\ \mathbb{Q} & \end{array}$$

<u>Prop</u>. 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.

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

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

<u>Next time</u>: Get a surjection

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