38 The Frobenius Endomorphism

We keep our setup: $p$ lies above $p$ in $\mathcal{O}_K$. Picture:

Assume now that $p$ is unramified, so we have our isomorphism

\[ D_p \stackrel{\theta}{\to} \text{Gal}((\mathcal{O}_K/p)/\mathbb{F}_p). \]

Recall that $\theta$ sends $\sigma \in D_p$ to the map

\[ \theta(\sigma): \alpha \pmod{p} \mapsto \sigma(\alpha) \pmod{p}. \]

Since $\sigma$ is supposed to fix $p$, this is well-defined.

Again, we already know $\text{Gal}((\mathcal{O}_K/p)/\mathbb{F}_p)$, according to the string of isomorphisms

\[ \text{Gal}((\mathcal{O}_K/p)/\mathbb{F}_p) \cong \text{Gal}(\mathbb{F}_p^f/\mathbb{F}_p) \cong \langle x \mapsto x^p \rangle \cong \mathbb{Z}_f. \]

If we take the generator of $\mathbb{Z}_f$, we get the so-called Frobenius element, which will turn out to be absurdly powerful.

Throughout this chapter $K/\mathbb{Q}$ is a Galois extension with Galois group $G$, $p$ is an unramified rational prime in $K$, and $p$ is a prime above it.

38.1 Frobenius Endomorphisms

Let me draw the picture before I say what I’m going to do:

\[ G = \text{Gal}(K/\mathbb{Q}) \quad \mathbb{Z}_f = \langle T \mid T^f = 1 \rangle \]

The point is to take the generator in $\mathbb{Z}_f$ and see who it goes to in $G$. By the definition of $\theta$, we distinguish this element as $\text{Frob}_p$. The following theorem makes this all precise:

342
Chapter 38. The Frobenius Endomorphism

**Theorem 38.1.1 (The Frobenius Element)**

Assume $K/Q$ is Galois with Galois group $G$. Let $p$ be a rational prime unramified in $K$, and $\mathfrak{p}$ a prime above it. There is a unique element $\text{Frob}_p \in G$ with the property that

$$\text{Frob}_p(\alpha) \equiv \alpha^p \pmod{\mathfrak{p}}.$$  

It is called the Frobenius endomorphism at $p$, and has order $f$.

**Proof.** First, observe:

**Question 38.1.2.** Show that such an element must be in $D_p$.

Now $\theta(\sigma)$ has the property if and only if it equals $T$, so everything is clear from the isomorphism $\theta$. \(\square\)

The uniqueness part is pretty important: it allows us to show that a given $\sigma$ is actually equal to the generator of $\text{Gal}(K/Q)$ by just observing that it satisfies the above functional equation. We'll use this more than once in the proof of quadratic reciprocity.

**Example 38.1.3 (Frobenius Elements of the Gaussian Integers)**

Let’s actually compute some Frobenius elements for $K = \mathbb{Q}(i)$, which has $\mathcal{O}_K = \mathbb{Z}[i]$. This is a Galois extension, with $G = \mathbb{Z}_2^\times$, corresponding to the identity and complex conjugation.

(a) Let $p \equiv 1 \pmod{4}$. Then $(p) = (a + bi)(a - bi)$ in $\mathbb{Z}[i]$; set $\mathfrak{p} = a + bi$. so $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_p$. So in this case the Galois group $\text{Gal}((\mathcal{O}_K/\mathfrak{p})/\mathbb{F}_p)$ is trivial, and as predicted we have $D_p$ trivial as well. Thus $\text{Frob}_p = \text{id}$.

(b) Now let $p \equiv 3 \pmod{4}$, and let $\mathfrak{p} = (p)$. Then $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_p[i] \cong \mathbb{F}_{p^2}$, and the Galois group has order 2; accordingly, $D_p$ has order 2, and its generator is $\text{Frob}_p$.

So $\sigma = \text{Frob}_p$ has order 2, and it must be complex conjugation. We can see this directly as well: $\sigma$ is the unique element such that

$$(a + bi)^p \equiv \sigma(a + bi) \pmod{\mathfrak{p}}$$

in $\mathbb{Z}[i]$. For $a = 0$ and $b = 1$, we get $\sigma(i) \equiv i^p \equiv -i \pmod{\mathfrak{p}}$, and so $\sigma$ must be complex conjugation.

### 38.2 Conjugacy Classes

Now suppose $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are two primes above an unramified rational prime $p$. Then we can define $\text{Frob}_{\mathfrak{p}_1}$ and $\text{Frob}_{\mathfrak{p}_2}$. Let $\sigma \in \text{Gal}(K/Q)$ be such that

$$\sigma(\mathfrak{p}_1) = \mathfrak{p}_2$$

possible since the Galois group acts transitively. We claim that

$$\text{Frob}_{\mathfrak{p}_2} = \sigma \circ \text{Frob}_{\mathfrak{p}_1} \circ \sigma^{-1}.$$  

Note that this is an equation in $G$.

**Question 38.2.1.** Prove this.
More generally, for a given unramified rational prime \( p \), we obtain the following:

**Theorem 38.2.2 (Conjugacy Classes in Galois Groups)**

The set

\[
\{ \text{Frob}_p \mid p \text{ above } p \}
\]

is one of the conjugacy classes of \( G \).

**Proof.** We’ve used the fact that \( G = \text{Gal}(K/\mathbb{Q}) \) is transitive to show that \( \text{Frob}_{p_1} \) and \( \text{Frob}_{p_2} \) are conjugate if they both lie above \( p \); hence it’s contained in some conjugacy class. So it remains to check that for any \( p, \sigma \), we have \( \sigma \circ \text{Frob}_p \circ \sigma^{-1} = \text{Frob}_{p'} \) for some \( p' \). For this, just take \( p' = \sigma p \). Hence the set is indeed a conjugacy class. \( \square \)

In summary,

\( \text{Frob}_p \) is determined up to conjugation by the prime \( p \) from which \( p \) arises.

So even the Gothic letters look scary, the content of \( \text{Frob}_p \) really just comes from the more friendly-looking rational prime \( p \).

**Example 38.2.3 (Frobenius Elements in \( \mathbb{Q}(\sqrt[3]{2}, \omega) \))**

With those remarks, here is a more involved example of a Frobenius map. Let \( K = \mathbb{Q}(\sqrt[3]{2}, \omega) \) be the splitting field of

\[
t^3 - 2 = (t - \sqrt[3]{2})(t - \omega \sqrt[3]{2})(t - \omega^2 \sqrt[3]{2}).
\]

We’ve seen in an earlier example that

\[
\mathcal{O}_K \cong \mathbb{Z}[\varepsilon] \quad \text{where} \quad \varepsilon \text{ is a root of } t^6 + 3t^5 - 5t^3 + 3t + 1.
\]

We factor 5 as the prime

\[
(5) = (5, \varepsilon^2 + \varepsilon + 2)(5, \varepsilon^2 + 3\varepsilon + 3)(5, \varepsilon^2 + 4\varepsilon + 1).
\]

Take the first one, \( \mathfrak{P} = (5, \varepsilon^2 + \varepsilon + 2) \). It follows that

\[
\mathcal{O}_K/\mathfrak{P} \cong \mathbb{F}_5[\varepsilon]/(\varepsilon^2 + \varepsilon + 2).
\]

As this field has \( 5^2 = 25 \) elements, the Galois group of this guy over \( \mathbb{F}_5 \) is order 2. Thus \( D_p \cong \mathbb{Z}_2^k \) as well and \( \sigma = \text{Frob}_\mathfrak{P} \) will have order 2.

Note that \( \text{Gal}(K/\mathbb{Q}) \cong S_3 \) is just the 6! = 6 permutations of the three roots \( \{ \sqrt[3]{2}, \omega \sqrt[3]{2}, \omega^2 \sqrt[3]{2} \} \). Exactly three of these have order 2, and they correspond to the three prime ideals of 5; each of the three Frobenius elements from 5 correspond to fixing one of the roots and swapping the other two. In still other words, the conjugacy class associated to 5 is the cycle type \((\bullet)(\bullet)\) in \( S_3 \).

### 38.3 Cheboratev Density Theorem

This naturally begs the question: can we represent every conjugacy class in this way? In other words, is every element of \( G \) equal to \( \text{Frob}_p \) for some \( p \)?
Miraculously, not only is the answer “yes”, but in fact it does so in the nicest way possible: the Frob\(_p\)’s are “equally distributed” when we pick a random \(p\).

**Theorem 38.3.1** (Cheboratev Density Theorem over \(\mathbb{Q}\))

Let \(C\) be a conjugacy class of \(G = \text{Gal}(K/\mathbb{Q})\). The density of (unramified) primes \(p\) such that \(\{\text{Frob}_p \mid p \text{ above } p\} = C\) is exactly \(|C| / |G|\). In particular, for any \(\sigma \in G\) there are infinitely many rational primes \(p\) with \(p \text{ above } p\) so that \(\text{Frob}_p = \sigma\).

![Figure 38.1: From a pretty excellent movie...](image)

By density, I mean that the proportion of primes \(p \leq x\) that work approaches \(|C| / |G|\) as \(x \to \infty\). Note that I’m throwing out the primes that ramify in \(K\). This is no issue, since the only primes that ramify are those dividing \(\Delta_K\), and we can throw those out. In other words, if I pick a random prime \(p\) and look at the resulting conjugacy class, it’s a lot like throwing a dart at \(G\): the probability of hitting any conjugacy class depends just on the size of the class.

![Diagram](image)

**Remark 38.3.2.** Happily, this theorem also works if we replace \(K/\mathbb{Q}\) with any Galois extension \(K/F\); in that case we replace “\(p\) over \(p\)” with “\(\mathfrak{p}\) over \(p\)”.

In that case, we use \(N(p) \leq x\) rather than \(p \leq x\) as the way to define density.

### 38.4 Example: Frobenius Elements of Cyclotomic Fields

Let \(q\) be a prime, and consider \(L = \mathbb{Q}(\zeta_q)\), with \(q\) a primitive \(q\)th root of unity. You should recall from various starred problems that
• $\Delta_L = \pm q^{n-2}$,
• $\mathcal{O}_L = \mathbb{Z}[\zeta_q]$, and
• The map $\sigma_n : \zeta_q \mapsto \zeta_q^n$ is an automorphism of $L$ whenever $\gcd(n, q) = 1$, and depends only on $n \pmod{q}$. In other words, the automorphisms of $L/\mathbb{Q}$ just shuffle around the $q$th roots of unity. In fact the Galois group consists exactly of the elements $\{\sigma_n\}$, namely

$$\text{Gal}(L/\mathbb{Q}) = \{\sigma_n \mid n \not\equiv 0 \pmod{q}\}.$$  

As a group,

$$\text{Gal}(L/\mathbb{Q}) = \mathbb{Z}_q^\times \cong \mathbb{Z}_{q-1}.$$  

This is surprisingly nice, because **elements of Gal(L/\mathbb{Q}) look a lot like Frobenius endomorphism already**. So we shouldn’t be surprised if the Frobenius endomorphisms of Gal(L/\mathbb{Q}) have a concrete description.

Let $p$ be a rational prime other than $q$, so $p$ doesn’t ramify (since $p \nmid \Delta_L$). Then $p$ is above it, and there is a Frobenius element $\text{Frob}_p$ uniquely determined by the property

$$\text{Frob}_p(\alpha) = \alpha^p \pmod{p}.$$  

**Lemma 38.4.1 (Cyclotomic Frobenius Elements)**

In the cyclotomic setting,

$$\text{Frob}_p = \sigma_p.$$  

**Proof.** We know $\text{Frob}_p(\alpha) \equiv \alpha^p \pmod{p}$ by definition, but also that $\text{Frob}_p = \sigma_n$ for some $n$. We want $n = p$, since $\sigma_n(\zeta_q)^n = \zeta_q^n$ by definition it would be very weird if this wasn’t true!

Given $\zeta_q^n \equiv \zeta_q^p \pmod{p}$, it suffices to prove that the $q$th roots of unity are distinct mod $p$. Look at the polynomial $F(x) = x^q - 1$ in $\mathbb{Z}[\zeta_p]/p \cong F_p$. Its derivative is

$$F'(x) = qx^{q-1} \not\equiv 0 \pmod{p}$$  

(since $F_p$ has characteristic $p \nmid q$). The only root of $F'$ is zero, hence $F$ has no double roots mod $p$.  

\[\square\]

**38.5 Frobenius Elements Behave Well With Restriction**

Consider the following setup, where $L/\mathbb{Q}$ and $K/\mathbb{Q}$ are both Galois extensions:

$$\begin{align*}
L & \supset \mathfrak{p} \quad \text{--------} \quad \text{Frob}_p \in \text{Gal}(L/\mathbb{Q}) \\
K & \supset \mathfrak{p} \quad \text{--------} \quad \text{Frob}_p \in \text{Gal}(K/\mathbb{Q}) \\
\mathbb{Q} & \supset (p)
\end{align*}$$
Here \( p \) is above \( (p) \) and \( \mathfrak{p} \) is above \( p \). We may define
\[
\text{Frob}_p : K \to K \quad \text{and} \quad \text{Frob}_{\mathfrak{p}} : L \to L
\]
and want to know how these are related.

**Theorem 38.5.1** (Restrictions of Frobenius Elements)
Assume \( L/\mathbb{Q} \) and \( K/\mathbb{Q} \) are both Galois. The restriction of \( \text{Frob}_{\mathfrak{p}} \) to \( K \) is \( \text{Frob}_p \), id est for every \( \alpha \in K \),
\[
\text{Frob}_p(\alpha) = \text{Frob}_{\mathfrak{p}}(\alpha).
\]

**Proof.** We know
\[
\text{Frob}_{\mathfrak{p}}(\alpha) \equiv \alpha^p \pmod{\mathfrak{p}} \quad \forall \alpha \in \mathcal{O}_L
\]
from the definition.

**Question 38.5.2.** Deduce that
\[
\text{Frob}_{\mathfrak{p}}(\alpha) \equiv \alpha^p \pmod{p} \quad \forall \alpha \in \mathcal{O}_K.
\]
(This is weaker than the previous statement in two ways!)
Thus \( \text{Frob}_{\mathfrak{p}} \) restricted to \( \mathcal{O}_K \) satisfies the characterizing property of \( \text{Frob}_p \).

In short, the point of this section is that

Frobenius elements upstairs restrict to Frobenius elements downstairs.

### 38.6 Application: Quadratic Reciprocity

We now aim to prove the following result from elementary number theory.

**Theorem 38.6.1** (Quadratic Reciprocity)
Let \( p \) and \( q \) be distinct odd primes. Then
\[
\left( \frac{p}{q} \right) \left( \frac{q}{p} \right) = (-1)^\frac{p-1}{2} \cdot \frac{q-1}{2}.
\]

**Step 1: Setup**
For this proof, we first define
\[
L = \mathbb{Q}(\zeta_q)
\]
where \( \zeta_q \) is a primitive \( q \)th root of unity. Then \( L/\mathbb{Q} \) is Galois, with Galois group \( G \).

**Question 38.6.2.** Show that \( G \) has a unique subgroup \( H \) of order two.

In fact, we can describe it exactly: viewing \( G \cong \mathbb{Z}_q^* \), we have
\[
H = \{ \sigma_n \mid n \text{ quadratic residue mod } q \}.
\]
By the Fundamental Theorem of Galois Theory, there ought to be a degree 2 extension of \( \mathbb{Q} \) inside \( \mathbb{Q}(\zeta_q) \) (that is, a quadratic field). Call it \( \mathbb{Q}(\sqrt{q^*}) \), for \( q^* \) squarefree:

\[
L = \mathbb{Q}(\zeta_q) \xrightarrow{\varphi} \{1\} \\
\xrightarrow{\varphi^{-1}} \\
K = \mathbb{Q}(\sqrt{q^*}) \xrightarrow{\psi} H \\
\xrightarrow{\psi^{-2}} \\
\mathbb{Q} \xrightarrow{G}
\]

**Exercise 38.6.3.** Note that if a rational prime \( \ell \) ramifies in \( K \), then it ramifies in \( L \).

Use this to show that

\[
q^* = \pm q \text{ and } q^* \equiv 1 \pmod{4}.
\]

Together these determine the value of \( q^* \).

**Step 2: Reformulation**

Now we are going to prove:

**Theorem 38.6.4 (Quadratic Reciprocity, Equivalent Formulation)**

For distinct odd primes \( p, q \) we have

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

**Exercise 38.6.5.** Using the fact that \( \left( \frac{1}{p} \right) = (-1)^{\frac{p-1}{2}} \), show that this is equivalent to quadratic reciprocity as we know it.

We look at the rational prime \( p \) in \( \mathbb{Z} \). Either it splits into two in \( K \) or is inert; either way let \( \mathfrak{p} \) be a prime factor in the resulting decomposition (so \( \mathfrak{p} \) is either \( p \cdot \mathcal{O}_K \) in the inert case, or one of the primes in the split case). Then let \( \mathfrak{P} \) be above \( \mathfrak{p} \). It could possibly also split in \( K \): the picture looks like

\[
\mathcal{O}_L = \mathbb{Z}[\zeta_q] \supset \mathfrak{P} \quad \cdots \quad \mathbb{Z}[\zeta_{p^2}] / \mathfrak{P} \cong \mathbb{F}_{p^2} \\
\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{q^*}}{2}] \supset \mathfrak{p} \quad \cdots \quad \mathbb{F}_p \text{ or } \mathbb{F}_{p^2} \\
\mathbb{Z} \supset (p) \quad \cdots \quad \mathbb{F}_p
\]

**Question 38.6.6.** Why is \( p \) not ramified in either \( K \) or \( L \)?

---

\(^1\) Actually, it is true in general that given a tower \( L/K/\mathbb{Q} \), we have \( \Delta_K \) divides \( \Delta_L \).
**Step 3: Introducing the Frobenius**

Now, we take the Frobenius $\sigma_p = \text{Frob}_p \in \text{Gal}(L/\mathbb{Q})$.

We claim that $\text{Frob}_p \in H \iff p$ splits in $K$.

To see this, note that $\text{Frob}_p$ is in $H$ if and only if it acts as the identity on $K$. But $\text{Frob}_p$ restricted to $K$ is $\text{Frob}_p$! So

$$\text{Frob}_p \in H \iff \text{Frob}_p = \text{id}_K.$$  

So we simply note that $\text{Frob}_p$ has order 1 if $p$ splits (and $p$ has inertial degree 1) and order 2 if $p$ is inert (hence $p = p \cdot O_K$ has inertial degree 2). After all, $\text{Frob}_p$ corresponds to the generator of

$$\text{Gal}((O_K/p)/\mathbb{F}_p) \cong \text{Gal}(\mathbb{F}_p/p) \text{ or } \text{Gal}(\mathbb{F}_p^2/p)$$

according to whether $p$ splits or is inert, respectively.

**Finishing Up**

We already know by Lemma 38.4.1 that $\text{Frob}_p = \sigma_p \in H$ if and only if $p$ is a quadratic residue. On the other hand,

**Exercise 38.6.7.** Show that $p$ splits in $O_K = \mathbb{Z}[\frac{1}{2}(1 + \sqrt{q^*})]$ if and only if $\left(\frac{q^*}{p}\right) = 1$.  
(Use the factoring algorithm. You need the fact that $p \neq 2$ here.)

In other words

$$\left(\frac{p}{q}\right) = 1 \iff \sigma_p \in H \iff p \text{ splits in } \mathbb{Z}\left[\frac{1}{2}(1 + \sqrt{q^*})\right] \iff \left(\frac{q^*}{p}\right) = 1.$$  

This completes the proof.

**38.7 Frobenius Elements Control Factorization**

*Prototypical example for this section:* $\text{Frob}_p$ controlled the splitting of $p$ in the proof of quadratic reciprocity; the same holds in general.

In the proof of quadratic reciprocity, we used the fact that Frobenius elements behaved well with restriction in order to relate the splitting of $p$ with properties of $\text{Frob}_p$.

In fact, there is a much stronger statement for any intermediate field $\mathbb{Q} \subseteq E \subseteq K$ which works even if $E/\mathbb{Q}$ is not Galois. It relies on the notion of a *factorization pattern*. Here is how it goes.

Set $n = [E : \mathbb{Q}]$, and let $p$ be a rational prime unramified in $K$. Then $p$ can be broken in $E$ as

$$p \cdot O_E = p_1 p_2 \cdots p_g$$

with inertial degrees $f_1, \ldots, f_g$; (these inertial degrees might be different since $E/\mathbb{Q}$ isn’t Galois). The numbers $f_1 + \cdots + f_g = n$ form a partition of the number $n$. For example, in the quadratic reciprocity proof we had $n = 2$, with possible partitions $1 + 1$ (if $p$ split) and $2$ (if $p$ was inert). We call this the *factorization pattern* of $p$ in $E$.  

349
Next, we introduce a Frobenius $\text{Frob}_P$ above $(p)$, all the way in $K$; this is an element of $G = \text{Gal}(K/\mathbb{Q})$. Then let $H$ be the group corresponding to the field $E$. Diagram:

\[
\begin{array}{cccc}
K & \xrightarrow{\text{Frob}_P} & \{1\} & \\
E & \xleftarrow{\text{Frob}_P} & H & \\
\cap & & \cap & \\
\cap & & \cap & \\
\mathbb{Q} & \xleftarrow{\text{Frob}_P} & G & (p)
\end{array}
\]

Then $\text{Frob}_P$ induces a permutation of the $n$ left cosets $gH$ by left multiplication (after all, $\text{Frob}_P$ is an element of $G$ too!). Just as with any permutation, we may look at the resulting cycle decomposition, which has a natural “cycle structure”: a partition of $n$.

\[
\begin{array}{cccc}
g &=& \text{Frob}_P \\
g_1 H & \times g & & g_4 H \\
g_2 H & \times g & & g_5 H \\
g_3 H & \times g & & g_6 H \\
3 & & & 1
\end{array}
\]

\[
n = 7 = 3 + 4
\]

The theorem is that these coincide:

**Theorem 38.7.1 (Frobenius Elements Control Decomposition)**

Let $\mathbb{Q} \subseteq E \subseteq K$ an extension of number fields and assume $K/\mathbb{Q}$ is Galois (though $E/\mathbb{Q}$ need not be). Pick an unramified rational prime $p$; let $G = \text{Gal}(K/\mathbb{Q})$ and $H$ the corresponding intermediate subgroup. Finally, let $\mathfrak{P}$ be a prime above $p$ in $K$.

Then the factorization pattern of $p$ in $E$ is given by the cycle structure of $\text{Frob}_\mathfrak{P}$ acting on the left cosets of $H$.

Often, we take $E = K$, in which case this is just asserting that the decomposition of the prime $p$ is controlled by a Frobenius element over it.

An important special case is when $E = \mathbb{Q}(\alpha)$, because as we will see it is let us determine how the minimal polynomial of $\alpha$ factors modulo $p$. To motivate this, let’s go back a few chapters and think about the Factoring Algorithm.

Let $\alpha$ be an algebraic integer and $f$ its minimal polynomial (of degree $n$). Set $E = \mathbb{Q}(\alpha)$ (which has degree $n$ over $\mathbb{Q}$). Suppose we’re lucky enough that $\mathcal{O}_E = \mathbb{Z}[\alpha]$; i.e. that $E$ is monogenic. Then we know by the Factoring Algorithm, to factor any $p$ in $E$, all we have to do is factor $f$ modulo $p$, since if $f = f_1^{e_1} \cdots f_g^{e_g} \pmod{p}$ then we have

\[
(p) = \prod_i p_i = \prod_i (f_i(\alpha), p)^{e_i}
\]
This gives us complete information about the ramification indices and inertial degrees; the $e_i$ are the ramification indices, and $\deg f_i$ are the inertial degrees (since if $O_E/p_i \cong \mathbb{F}_p[X]/(f_i(X)))$.

In particular, if $p$ is unramified then all the $e_i$ are equal to 1, and we get

$$n = \deg f = \deg f_1 + \deg f_2 + \cdots + \deg f_g.$$ 

Once again we have a partition of $n$; we call this the factorization pattern of $f$ modulo $p$. So, to see the factorization pattern of an unramified $p$ in $O_E$, we just have to know the factorization pattern of the $f$ (mod $p$).

Turning this on its head, if we want to know the factorization pattern of $f$ (mod $p$), we just need to know how $p$ decomposes. And it turns out these coincide even without the assumption that $E$ is monogenic.

**Theorem 38.7.2** (Frobenius Controls Polynomial Factorization)

Let $\alpha$ be an algebraic integer with minimal polynomial $f$, and let $E = \mathbb{Q}(\alpha)$. Then for any prime $p$ unramified in the splitting field $K$ of $f$, the following coincide:

(i) The factorization pattern of $p$ in $E$.

(ii) The factorization pattern of $f$ (mod $p$).

(iii) The cycle structure associated to the action of $\text{Frob}_P \in \text{Gal}(K/\mathbb{Q})$ on the roots of $f$, where $\mathfrak{P}$ is above $p$ in $K$.

**Example 38.7.3** (Factoring $x^3 - 2$ (mod 5))

Let $\alpha = \sqrt[3]{2}$ and $f = x^3 - 2$, so $E = \mathbb{Q}(\sqrt[3]{2})$. Set $p = 5$ and let finally, let $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$ be the splitting field. Setup:

$$
\begin{align*}
K &= \mathbb{Q}(\sqrt[3]{2}, \omega) \\
\mathfrak{P} &= x^3 - 2 = (x - \sqrt[3]{2})(x - \sqrt[3]{2} \omega)(x - \sqrt[3]{2} \omega^2)
\end{align*}
$$

The three claimed objects now all have shape $2 + 1$:

(i) By the Factoring Algorithm, we have $(5) = (5, \sqrt[3]{2} - 3)(5, 9 + 3\sqrt[3]{2} + \sqrt[3]{4})$.

(ii) We have $x^3 - 2 \equiv (x - 3)(x^2 + 3x + 9)$ (mod 5).

(iii) We saw before that $\text{Frob}_\mathfrak{P} = (\bullet)(\bullet \bullet)$.

*Sketch of Proof.* Letting $n = \deg f$. Let $H$ be the subgroup of $G = \text{Gal}(K/\mathbb{Q})$ corre-
corresponding to $E$, so $[G : E] = n$. Pictorially, we have

We claim that (i), (ii), (iii) are all equivalent to

(iv) The pattern of the action of Frob on the $G/H$.

In other words we claim the cosets correspond to the $n$ roots of $f$ in $K$. Indeed $H$ is just the set of $\tau \in G$ such that $\tau(\alpha) = \alpha$, so there’s a bijection between the roots and the cosets $G/H$ by $\tau H \mapsto \tau(\alpha)$. Think of it this way: if $G = S_n$, and $H = \{\tau : \tau(1) = 1\}$, then $G/H$ has order $n!/(n-1)! = n$ and corresponds to the elements $\{1, \ldots, n\}$. So there is a natural bijection from (iii) to (iv).

The fact that (i) is in bijection to (iv) was the previous theorem, Theorem 38.7.1. The correspondence (i) $\iff$ (ii) is a fact of Galois theory, so we omit the proof here. \qed

All this can be done in general with $\mathbb{Q}$ replaced by $F$; for example, in [Le02].

### 38.8 Example Application: IMO 2003 Problem 6

As an example of the power we now have at our disposal, let’s prove:

**Problem 6.** Let $p$ be a prime number. Prove that there exists a prime number $q$ such that for every integer $n$, the number $n^p - p$ is not divisible by $q$.

We will show, much more strongly, that there exist infinitely many primes $q$ such that $X^p - p$ is irreducible.

**Solution.** Okay! First, we draw the tower of fields

$$\mathbb{Q} \subseteq \mathbb{Q}^{\sqrt[p]{p}} \subseteq K$$

where $K$ is the splitting field of $f(x) = x^p - p$. Let $E = \mathbb{Q}^{\sqrt[p]{p}}$ for brevity and note it has degree $[E : \mathbb{Q}] = p$. Let $G = \text{Gal}(K/\mathbb{Q})$.

**Question 38.8.1.** Show that $p$ divides the order of $G$. (Look at $E$.)
Hence by Cauchy’s Theorem (Problem 13A*, which is a purely group-theoretic fact) we can find a \( \sigma \in G \) of order \( p \). By Cheboratev, there exists infinitely many rational (unramified) primes \( q \neq p \) and primes \( \mathfrak{Q} \subseteq \mathcal{O}_K \) above \( q \) such that \( \text{Frob}_\mathfrak{Q} = \sigma \). (Yes, that’s an uppercase Gothic \( Q \). Sorry.)

We claim that all these \( q \) work.

By Theorem 38.7.2, the factorization of \( f \) (mod \( q \)) is controlled by the action of \( \sigma = \text{Frob}_\mathfrak{Q} \) on the roots of \( f \). But \( \sigma \) has prime order \( p \) in \( G \)! So all the lengths in the cycle structure have to divide \( p \). Thus the possible factorization patterns of \( f \) are

\[
p = \underbrace{1 + 1 + \cdots + 1}_{p \text{ times}} \quad \text{or} \quad p = p.
\]

So we just need to rule out the \( p = 1 + \cdots + 1 \) case now: this only happens if \( f \) breaks into linear factors mod \( q \). Intuitively this edge case seems highly unlikely (are we really so unlucky that \( f \) factors into linear factors when we want it to be irreducible?). And indeed this is easy to see: this means that \( \sigma \) fixes all of the roots of \( f \) in \( f \), but that means \( \sigma \) fixes \( K \), and hence is the identity of \( G \), contradiction.

\[\square\]

**Remark 38.8.2.** In fact \( K = \mathbb{Q}(\sqrt[p]{p}, \zeta_p) \), and \( |G| = p(p - 1) \). With a little more group theory, we can show that in fact the density of primes \( q \) that work is \( \frac{1}{p} \).

### 38.9 Problems to Think About

**Problem 38A.** Show that for an odd prime \( p \),

\[
\left( \frac{2}{p} \right) = (-1)^{\frac{p - 1}{2}}.
\]

**Problem 38B.** Let \( f \) be a nonconstant polynomial with integer coefficients. Suppose \( f \) (mod \( p \)) splits completely into linear factors for all sufficiently large primes \( p \). Show that \( f \) splits completely into linear factors.

**Problem 38C† (Dirichlet’s Theorem on Arithmetic Progressions).** Let \( a \) and \( m \) be relatively prime positive integers. Show that the density of primes \( p \equiv a \) (mod \( m \)) is exactly \( \frac{1}{\phi(m)} \).

**Problem 38D.** Let \( n \) be an odd integer which is not a prime power. Show that the \( n \)th cyclotomic polynomial is not irreducible modulo any rational prime.