Frobenius map/automorphism

Artin map/automorphism

Dedekind rings.

The picture:
**Corollary:** For abelian $K/k$, the decomposition subfield $K^\mathfrak{P}$ is the maximal subfield of $K$ (containing $k$) in which $p$ splits completely.

**Proof:** With $\sigma_1, \ldots, \sigma_n$ representatives for $G/G_\mathfrak{P}$, by transitivity, $\sigma_j \mathfrak{P}$ are distinct, and are all the primes over $p$. The abelian-ness implies that the decomposition subfields $K^\mathfrak{P}$ for the $\sigma_j \mathfrak{P}$ are all the same.

Let $q = \mathfrak{P} \cap K^\mathfrak{P}$. From above, $\mathfrak{P}$ is the only prime over $q$, and $\sigma_j \mathfrak{P}$ is the only prime over $\sigma_j q$, and the latter must be distinct. Since $[K : k] = |G| = |G_\mathfrak{P}| \cdot n$, necessarily $p$ splits completely in $K^\mathfrak{P}$.

Conversely, with $E$ an intermediate field in which $p$ splits completely, $G_\mathfrak{P}$ fixes $\mathfrak{P} \cap E$. The hypothesis that $p$ splits completely in $E$ implies that the decomposition subgroup of $\mathfrak{P} \cap E$ in Gal$(E/k)$ is *trivial*. That is, the restriction of $G_\mathfrak{P}$ to $E$ is trivial, so $G_\mathfrak{P} \subset$ Gal$(K/E)$. ///
The distinguishing feature of **number fields** (finite extensions of \( \mathbb{Q} \)) and **function fields** (finite extensions of \( \mathbb{F}_p(x) \)), and their completions, is that their **residue fields are finite**.

All finite extensions of finite fields are **cyclic** (Galois).

There is a canonical generator, the **Frobenius automorphism** \( x \rightarrow x^q \) of the Galois group of **any** extension of \( \mathbb{F}_q \).

Given a prime \( p \) and \( \mathfrak{p} \) lying over it in a Galois extension \( K/k \) of number fields or functions fields, with residue field extension \( \tilde{\kappa}/\kappa \), with \( \kappa \approx \mathbb{F}_q \), the **Frobenius map/automorphism** in \( G_{\mathfrak{p}} \) is anything that maps to \( x \rightarrow x^q \).

**Artin map/automorphism** is Frobenius for **abelian** extensions.

The point is that, by transitivity of Galois on primes \( \mathfrak{p} \) lying over \( p \), in an **abelian** extension all decomposition groups \( G_{\mathfrak{p}} \) are the same subgroup, so the Frobenius element of \( \text{Gal}(K/k) \) does not depend on the choice of \( \mathfrak{p} \) over \( p \).
A **fractional ideal** \( \mathfrak{a} \) of \( \mathfrak{o} \) in its fraction field \( k \) is an \( \mathfrak{o} \)-submodule of \( k \) such that there is \( 0 \neq c \in \mathfrak{o} \) such that \( c\mathfrak{a} \subseteq \mathfrak{o} \).

**Examples:** Fractional ideals of \( \mathbb{Z} \) are \( \mathbb{Z} \cdot r \) for \( r \in \mathbb{Q} \).

\( \mathbb{Z} \)-submodules of \( \mathbb{Q} \) requiring infinitely-many generators are not fractional ideals. E.g., neither the localization \( \mathbb{Z}_{(p)} \), nor the localization

\[
\bigcup_{\ell \geq 1} \frac{1}{p^\ell} \cdot \mathbb{Z}
\]  

(not a fractional ideal)

**Theorem:** In a Noetherian, integrally closed integral domain \( \mathfrak{o} \) in which every non-zero prime ideal is maximal, every non-zero ideal is **uniquely a product of prime ideals**, and the non-zero fractional ideals form a **group** under multiplication. [Below...]

**Dedekind domains** are Noetherian, integrally-closed integral domains in which every non-zero prime ideal is maximal. The **ideal class group** \( I_k = I_\mathfrak{o} \) is the group of non-zero fractional ideals modulo **principal** fractional ideals.
Also: Dedekind domains are characterized by the fact that their ideals are finitely-generated projective modules. [Proof later.]

An $R$-module $P$ is projective when any diagram

\[
\begin{array}{ccc}
B & \longrightarrow & C \\
\uparrow & & \uparrow \\
P & & \\
\end{array}
\to 0
\]

(with $B \to C \to 0$ exact)

admits at least one extension to a commutative diagram

\[
\begin{array}{ccc}
B & \longrightarrow & C \\
\downarrow & & \downarrow \\
P & & \\
\end{array}
\to 0
\]

*Free* modules are projective, but over non-PIDs there are more.
While we’re here: an $R$-module $I$ is *injective* when any diagram

\[
\begin{array}{ccc}
0 & \longrightarrow & A \\
\downarrow & & \downarrow \\
& I & \\
\end{array} \quad \longrightarrow \quad \begin{array}{ccc}
& & B \\
& \downarrow & \\
& & \downarrow \\
\end{array}
\]
(with $0 \to A \to B$ exact)

admits at least one extension to a commutative diagram

\[
\begin{array}{ccc}
0 & \longrightarrow & A \\
\downarrow & & \downarrow \\
I & \searrow & \\
\end{array} \quad \longrightarrow \quad \begin{array}{ccc}
& & B \\
& \downarrow & \\
& & \downarrow \\
\end{array}
\]
(with $0 \to A \to B$ exact)

Baer showed that, for example, *divisible* $\mathbb{Z}$-modules are injective.
The **structure theorem for finitely-generated modules** over PIDs, over Dedekind domains, is **Steinitz’ theorem**: 

A finitely-generated module $M$ over a Dedekind domain $\mathfrak{o}$ is

$$M \cong \mathfrak{o}/a_1 \oplus \ldots \oplus \mathfrak{o}/a_n \oplus \mathfrak{o}^r \oplus \mathfrak{a}$$

where $a_1|\ldots|a_n$ are uniquely-determined non-zero ideals, the rank $r$ of the free part $\mathfrak{o}^r$ is uniquely determined, and the isomorphism class of the ideal $\mathfrak{a}$ is uniquely determined.

[This is often omitted from algebraic number theory books. See Milnor’s *Algebraic K-theory*, or Cartan-Eilenberg.]

That is, the ideal class group is the torsion part of the $K$-group $K_0(\mathfrak{o}) = \text{projective finitely-generated } \mathfrak{o}\text{-modules, with tensor product, modulo free.}$
\textit{Proof:} [van der Waerden, Lang] Let \( \mathfrak{o} \) be a Noetherian integral domain, integrally closed in its field of fractions, and every non-zero prime ideal is maximal.

First: given non-zero ideal \( \mathfrak{a} \), there is a product of non-zero prime ideals \textit{contained in} \( \mathfrak{a} \). If not, by Noetherian-ness there is a \textit{maximal} ideal \( \mathfrak{a} \) failing to contain a product of primes, and \( \mathfrak{a} \) is not prime. Thus, there are \( b, c \in \mathfrak{o} \) neither in \( \mathfrak{a} \) such that \( bc \in \mathfrak{a} \). Thus, \( b = \mathfrak{a} + \mathfrak{o}b \) and \( c = \mathfrak{a} + \mathfrak{o}c \) are strictly larger than \( \mathfrak{a} \), and \( bc \subseteq \mathfrak{a} \).

Since \( \mathfrak{a} \) was maximal among ideals not containing a product of primes, both \( b, c \) contain such products. But then their product \( bc \subseteq \mathfrak{a} \) does, contradiction.
Second: for maximal $m$, the $o$-module $m^{-1} = \{x \in k : xm \subset o\}$ is strictly larger than $o$. Certainly $m^{-1} \supset o$, since $m$ is an ideal. We claim that $m^{-1}$ is strictly larger than $o$. Indeed, for $m \in m$ and a (smallest possible) product of primes $p_j$ such that

$$p_1 \ldots p_n \subset m o$$

Since $mo \subset m$ and $m$ is prime, $p_j \subset m$ for at least one $p_j$, say $p_1$. Since every (non-zero) prime is maximal, $p_1 = m$.

By minimality, $p_2 \ldots p_n \not\subset m o$. That is, there is $y \in p_2 \ldots p_n$ but $y \not\in mo$, or $m^{-1} y \not\in o$. But $ym = yp_1 \subset m o$, so $m^{-1} y m \subset o$, and $m^{-1} y \in m^{-1}$ but not in $o$. 
Third: maximal $m$ in $\mathfrak{o}$ is invertible. By this point, $m \subset m^{-1}m \subset \mathfrak{o}$. By maximality of $m$, either $m^{-1}m = m$ or $m^{-1}m = \mathfrak{o}$.

The Noetherian-ness of $\mathfrak{o}$ implies that $m$ is finitely-generated. A relation $m^{-1}m = m$ would show that $m^{-1}$ stabilizes a non-zero, finitely-generated $\mathfrak{o}$-module. Since $\mathfrak{o}$ is integrally closed in $k$, this would give $m^{-1} \subset \mathfrak{o}$, but we have seen otherwise. Thus, we have the inversion relation $m^{-1}m = \mathfrak{o}$ for maximal $m$.

Fourth: every non-zero ideal $a$ has inverse $a^{-1} = \{y \in k : ya \subset \mathfrak{o}\}$. If not, there is maximal $a$ failing this, and $a$ cannot be a maximal ideal, by the previous step. Thus, $a$ is properly contained in some maximal ideal $m$. Certainly $a \subset m^{-1}a \subset a^{-1}a \subset \mathfrak{o}$. Integral-closedness of $\mathfrak{o}$ and $m^{-1} \neq \mathfrak{o}$, $m \supset \mathfrak{o}$ show that $m^{-1}a \not\subset a$.

Thus, $m^{-1}a$ is strictly larger than $a$, so has an inverse $f$. Thus, $(fm^{-1}) \cdot a = f \cdot (m^{-1}a) = \mathfrak{o}$. That is, $fm^{-1}$ is an inverse for $a$, contradiction.

[cont’d]