Frobenius map/automorphism

Artin map/automorphism

Dedekind rings.

The picture:

$$
\begin{tikzcd}
K \arrow[r, dash, "\supset"] \arrow[dd, dash, "G_{\mathfrak{P}}"'] & \mathfrak{O} \arrow[r, dash, "\supset"] \arrow[dd, dash] \arrow[rrd] & \mathfrak{P} \arrow[dd, dash] & \\
 & & & \mathfrak{O}/\mathfrak{P} = \tilde{\kappa} \arrow[dd, dash, "G_{\mathfrak{P}}/I_{\mathfrak{P}}"] \\
K^{\mathfrak{P}} \arrow[r, dash, "\supset"] \arrow[dd, dash] & \mathfrak{O}^{\mathfrak{P}} \arrow[r, dash, "\supset"] \arrow[dd, dash] \arrow[rrd] & \mathfrak{q} = \mathfrak{P} \cap K^{\mathfrak{P}} \arrow[dd, dash] & \\
 & & & \mathfrak{O}^{\mathfrak{P}}/\mathfrak{q} \arrow[dd, dash, "="] \\
k \arrow[r, dash, "\supset"] & \mathfrak{o} \arrow[r, dash, "\supset"] \arrow[rrd] & \mathfrak{p} & \\
 & & & \mathfrak{o}/\mathfrak{p} = \kappa
\end{tikzcd}
$$

Corollary: For *abelian* K/k, the decomposition subfield $K^{\mathfrak{P}}$ is the maximal subfield of K (containing k) in which $\mathfrak{p}$ 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 $\mathfrak{p}$. The abelian-ness implies that the decomposition subfields $K^{\mathfrak{P}}$ for the $\sigma_j\mathfrak{P}$ are all the same.

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

Conversely, with E an intermediate field in which $\mathfrak{p}$ splits completely, $G_{\mathfrak{P}}$ fixes $\mathfrak{P} \cap E$. The hypothesis that $\mathfrak{p}$ splits completely in E implies that the decomposition subgroup of $\mathfrak{P} \cap E$ in $\mathrm{Gal}(E/k)$ is *trivial.* That is, the restriction of $G_{\mathfrak{P}}$ to E is trivial, so $G_{\mathfrak{P}} \subset \mathrm{Gal}(K/E)$. ///

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** $x \to x^q$ of the Galois group of *any* extension of $\mathbb{F}_q$.

Given a prime $\mathfrak{p}$ 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 $x \to x^q$.

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

The point is that, by transitivity of Galois on primes $\mathfrak{P}$ lying over $\mathfrak{p}$, in an *abelian* extension all decomposition groups $G_{\mathfrak{P}}$ are the same subgroup, so the Frobenius element of $\mathrm{Gal}(K/k)$ does not depend on the choice of $\mathfrak{P}$ over $\mathfrak{p}$.

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 $c\mathfrak{a} \subset \mathfrak{o}$.

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

$$\bigcup_{\ell \geq 1} \frac{1}{p^\ell} \cdot \mathbb{Z} \qquad\qquad (\textbf{not} \text{ a fractional ideal})$$

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

$$\begin{tikzcd} B \arrow[r] & C \arrow[r] & 0 \\ & P \arrow[u] & \end{tikzcd} \qquad \text{(with } B \to C \to 0 \text{ exact)}$$

admits at least one extension to a commutative diagram

$$\begin{tikzcd} B \arrow[r] & C \arrow[r] & 0 \\ & P \arrow[u] \arrow[ul, dashed] & \end{tikzcd}$$

Free modules are projective, but over non-PIDs there are more.

While we're here: an R-module I is *injective* when any diagram

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r] \arrow[d] & B \\ & I & \end{tikzcd} \qquad \text{(with } 0 \to A \to B \text{ exact)}$$

admits at least one extension to a commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r] \arrow[d] & B \arrow[dl, dashed] \\ & I & \end{tikzcd} \qquad \text{(with } 0 \to A \to B \text{ exact)}$$

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

$$M \approx \mathfrak{o}/\mathfrak{a}_1 \oplus \ldots \oplus \mathfrak{o}/\mathfrak{a}_n \oplus \mathfrak{o}^r \oplus \mathfrak{a}$$

where $\mathfrak{a}_1 | \ldots | \mathfrak{a}_n$ 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 $K_0(\mathfrak{o})$ = projective finitely-generated $\mathfrak{o}$-modules, with tensor product, modulo free.

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 *contained in* $\mathfrak{a}$. If not, by Noetherian-ness there is a *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, $\mathfrak{b} = \mathfrak{a} + \mathfrak{o}b$ and $\mathfrak{c} = \mathfrak{a} + \mathfrak{o}c$ are strictly larger than $\mathfrak{a}$, and $\mathfrak{bc} \subset \mathfrak{a}$.

Since $\mathfrak{a}$ was maximal among ideals not containing a product of primes, both $\mathfrak{b}, \mathfrak{c}$ contain such products. But then their product $\mathfrak{bc} \subset \mathfrak{a}$ does, contradiction.

Second: for maximal $\mathfrak{m}$, the $\mathfrak{o}$-module $\mathfrak{m}^{-1} = \{x \in k : x\mathfrak{m} \subset \mathfrak{o}\}$ is strictly larger than $\mathfrak{o}$. Certainly $\mathfrak{m}^{-1} \supset \mathfrak{o}$, since $\mathfrak{m}$ is an ideal. We claim that $\mathfrak{m}^{-1}$ is strictly larger than $\mathfrak{o}$. Indeed, for $m \in \mathfrak{m}$ and a (smallest possible) product of primes $\mathfrak{p}_j$ such that

$$\mathfrak{p}_1 \ldots \mathfrak{p}_n \subset m\mathfrak{o}$$

Since $m\mathfrak{o} \subset \mathfrak{m}$ and $\mathfrak{m}$ is prime, $\mathfrak{p}_j \subset \mathfrak{m}$ for at least one $\mathfrak{p}_j$, say $\mathfrak{p}_1$. Since every (non-zero) prime is maximal, $\mathfrak{p}_1 = \mathfrak{m}$.

By minimality, $\mathfrak{p}_2 \ldots \mathfrak{p}_n \not\subset m\mathfrak{o}$. That is, there is $y \in \mathfrak{p}_2 \ldots \mathfrak{p}_n$ but $y \notin m\mathfrak{o}$, or $m^{-1}y \notin \mathfrak{o}$. But $y\mathfrak{m} = y\mathfrak{p}_1 \subset m\mathfrak{o}$, so $m^{-1}y\mathfrak{m} \subset \mathfrak{o}$, and $m^{-1}y \in \mathfrak{m}^{-1}$ but not in $\mathfrak{o}$.

Third: maximal $\mathfrak{m}$ in $\mathfrak{o}$ is invertible. By this point, $\mathfrak{m} \subset \mathfrak{m}^{-1}\mathfrak{m} \subset \mathfrak{o}$. By maximality of $\mathfrak{m}$, either $\mathfrak{m}^{-1}\mathfrak{m} = \mathfrak{m}$ or $\mathfrak{m}^{-1}\mathfrak{m} = \mathfrak{o}$.

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

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

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

[cont'd]