More about *primes lying over...*

$\mathfrak{p}$ **splits completely** in K when there are $[K : k]$ distinct primes lying over $\mathfrak{p}$ in $\mathfrak{O}$.

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

Frobenius map/automorphism

Artin map/automorphism

... and **Dedekind rings**.

The picture is

$$
\begin{tikzcd}
K \arrow[r, dash, "\supset"] \arrow[dd, dash, "G_{\mathfrak{P}}"'] & \mathfrak{O} \arrow[r, dash, "\supset"] \arrow[dd, dash] \arrow[dr, shift left=0, to path={}, phantom] \arrow[drr] & \mathfrak{P} \arrow[dd, dash] & \\
 & & & \mathfrak{O}/\mathfrak{P} = \tilde{\kappa} \arrow[dd, dash] \\
K^{\mathfrak{P}} \arrow[r, dash, "\supset"] \arrow[dd, dash] & \mathfrak{O}^{\mathfrak{P}} \arrow[r, dash, "\supset"] \arrow[dd, dash] \arrow[drr] & \mathfrak{q} = \mathfrak{P} \cap K^{\mathfrak{P}} \arrow[dd, dash] & \\
 & & & \mathfrak{O}^{\mathfrak{P}}/\mathfrak{q} \arrow[dd, dash, "="', "\text{[pf below]}"] \\
k \arrow[r, dash, "\supset"] & \mathfrak{o} \arrow[r, dash, "\supset"] \arrow[drr] & \mathfrak{p} & \\
 & & & \mathfrak{o}/\mathfrak{p} = \kappa
\end{tikzcd}
$$

So far, we know that in the Galois case G is *transitive* on primes $\mathfrak{P}$ lying over $\mathfrak{p}$.

And the decomposition subfield $K^{\mathfrak{P}}$ (=fixed field of decomposition group $G_{\mathfrak{P}}$) is the smallest subfield of K such that $\mathfrak{P}$ is the only prime lying over $K^{\mathfrak{P}} \cap \mathfrak{P}$.

Claim: The inclusion $\mathfrak{o}/\mathfrak{p} \to \mathfrak{O}^{\mathfrak{P}}/\mathfrak{q}$ to the residue field attached to the decomposition field of $\mathfrak{P}$ is an *isomorphism.*

Proof: The induced map is indeed an *inclusion*, because

$$\mathfrak{p} \;=\; k \cap \mathfrak{P} \;=\; k \cap K^{\mathfrak{P}} \cap \mathfrak{P}$$

For surjectivity: for $\sigma \in G$ but not in $G_{\mathfrak{P}}$, $\sigma\mathfrak{P} \neq \mathfrak{P}$, and the prime ideal

$$\mathfrak{q}_\sigma \;=\; K^{\mathfrak{P}} \cap \sigma\mathfrak{P}$$

is not $\mathfrak{q}$, since $\mathfrak{P}$ is the only prime lying over $\mathfrak{q}$.

Thus, given $x \in \mathfrak{O}^{\mathfrak{P}}$, Sun-Ze's theorem gives $y \in \mathfrak{O}^{\mathfrak{P}}$ such that

$$\begin{cases} y = x \mod \mathfrak{q} \\ \\ y = 1 \mod \mathfrak{q}_\sigma \quad \text{(for all } \sigma \text{ not in } G_{\mathfrak{P}}) \end{cases}$$

Thus, certainly in the larger ring $\mathfrak{O}$

$$\begin{cases} y = x \mod \mathfrak{P} \\ \\ y = 1 \mod \sigma\mathfrak{P} \quad \text{(for all } \sigma \text{ not in } G_{\mathfrak{P}}) \end{cases}$$

That is, $\sigma y = 1 \bmod \mathfrak{P}$ for $\sigma \not\in G^{\mathfrak{P}}$. The Galois norm of y from $K^{\mathfrak{P}}$ to k is a product of y with images σy with $\sigma \not\in G^{\mathfrak{P}}$. Therefore,

$$N_k^{K^{\mathfrak{P}}} y = x \bmod \mathfrak{P}$$

The norm is in $\mathfrak{o}$, and the congruence holds mod $\mathfrak{q}$ since $x \in \mathfrak{O}^{\mathfrak{P}}$.

///

Claim: $\tilde{\kappa} = \mathfrak{O}/\mathfrak{P}$ is *normal* over $\kappa = \mathfrak{o}/\mathfrak{p}$, and $G_{\mathfrak{P}}$ *surjects* to $\mathrm{Gal}(\tilde{\kappa}/\kappa)$.

Proof: Let $\alpha \in \mathfrak{O}$ generate a separable subextension (mod $\mathfrak{P}$) of $\tilde{\kappa}$ over κ. The minimal polynomial of α over k has coefficients in $\mathfrak{o}$ because α is integral over $\mathfrak{o}$. Since K/k is Galois, f splits into linear factors $x - \alpha_i$ in $K[x]$. Then f mod $\mathfrak{P}$ factors into linear factors $x - \bar{\alpha}_i$ where $\bar{\alpha}_i$ is α_i mod $\mathfrak{P}$.

Thus, whatever the minimal polynomial of $\bar{\alpha}$ over κ, it factors into linear factors in $\tilde{\kappa}[x]$. That is, $\tilde{\kappa}/\kappa$ is normal, and

$$[\kappa(\bar{\alpha}) : \kappa] \;\leq\; [k(\alpha) : k] \;\leq\; [K : k]$$

By the theorem of the primitive element, the maximal separable subextension is of finite degree, bounded by $[K : k]$.

To prove surjectivity of the Galois group map, it suffices to consider the situation that $\mathfrak{P}$ is the only prime over $\mathfrak{p}$, from the discussion of the decomposition group and field above. Thus, $G = G_{\mathfrak{P}}$ and $K = K^{\mathfrak{P}}$.

By the theorem of the primitive element, there is α in $\mathfrak{O}$ with image $\bar{\alpha}$ mod $\mathfrak{P}$ generating the (maximal separable subextension of the) residue field extension $\tilde{\kappa}/\kappa$. Let f be the minimal polynomial of α over k, and $\overline{f}$ the reduction of f mod $\mathfrak{p}$.

Normality of K/k gives the factorization of $f(x)$ into linear factors $x - \alpha_i$ in $\mathfrak{O}[x]$, and this factorization reduces mod $\mathfrak{P}$ to a factorization into linear factors $x - \bar{\alpha}_i$ in $\tilde{\kappa}[x]$.

Automorphisms of $\tilde{\kappa}/\kappa$ are determined by their effect on $\bar{\alpha}$, and map $\bar{\alpha}$ to other zeros $\bar{\alpha}_i$ of $\overline{f}$. $\mathrm{Gal}(K/k)$ is *transitive* on the α_i, so is transitive on the $\bar{\alpha}_i$. This proves surjectivity. ///

The **inertia subgroup** is the kernel $I_{\mathfrak{P}}$ of $G_{\mathfrak{P}} \to \mathrm{Gal}(\tilde{\kappa}/\kappa)$, and the **inertia subfield** is the fixed field of $I_{\mathfrak{P}}$. (This is better called the 0^{th} **ramification** group...) For typical K/k, we'll see later that $I_{\mathfrak{P}}$ is *trivial* for most $\mathfrak{P}$.

Remark: For us, $\tilde{\kappa}/\kappa$ will almost always be *separable*.

A prime $\mathfrak{p}$ is **inert** in K/k (or in $\mathfrak{O}/\mathfrak{o}$) the degree of the residue field extension (for any prime lying over $\mathfrak{p}$) is equal to the global field extension degree: $[\tilde{\kappa} : \kappa] = [K : k]$.

Corollary: For *finite* residue field κ, existence of inert primes in K/k implies $\mathrm{Gal}(K/k)$ is *cyclic*.

Proof: Galois groups of finite extensions of finite fields are (separable and) cyclic. The degree equality requires that the map $G_{\mathfrak{P}} \to \mathrm{Gal}(\tilde{\kappa}/\kappa)$ be an *isomorphism*, and that $G = G_{\mathfrak{P}}$. ///

Examples:

In quadratic Galois extensions K/k, there is no obvious *obstacle* to primes being *inert*, since a group with 2 elements could easily surject to a group with 2 elements.

Remark: Lack of an obstacle does not prove *existence*... Indeed, in extensions of $\mathbb{C}(x)$ no prime stays prime, since the residue fields are all $\mathbb{C}$, which is already algebraically closed.

In non-abelian Galois extensions such as $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$, with ω a cube root of unity, *no* prime $p \in \mathfrak{o} = \mathbb{Z}$ can stay prime.

The Galois group of a cyclotomic extension $\mathbb{Q}(\omega)/\mathbb{Q}$ with ω an n^{th} root of unity is $(\mathbb{Z}/n)^\times$, which is *cyclic* only for n of the form $n = p^\ell$, $n = 2p^\ell$, for p an odd prime, and for $n = 4$ (from elementary number theory).

[*Examples,* cont'd]

We had already seen that $p \in \mathbb{Z}$ stays prime in $\mathbb{Q}(\omega)/\mathbb{Q}$ if and only if the n^{th} cyclotomic polynomial Φ_n is irreducible in $\mathbb{F}_p[x]$. This irreducibility is equivalent to n *not* dividing $p^d - 1$ for any $d < \deg \Phi_n$. This is equivalent to p being a *primitive root* (=generator) for $(\mathbb{Z}/n)^\times$.

Again, a *necessary* condition for cyclic-ness of $(\mathbb{Z}/n)^\times$ is that n be of the special forms $p^\ell, 2p^\ell, 4$.

But *Dirichlet's theorem* on primes in arithmetic progression is necessary to prove existence of *primes* equal mod n to a primitive root.

Quadratic reciprocity gives a congruence condition for quadratic extensions of $\mathbb{Q}$, and Dirichlet's theorem again gives *existence.*

$\mathfrak{p}$ **splits completely** in K when there are $[K : k]$ distinct primes lying over $\mathfrak{p}$ in $\mathfrak{O}$.

Examples:

In $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$ with square-free $D \in \mathbb{Z}$, odd p not dividing D with D a square mod p *split completely*: with $D = 2, 3 \bmod 4$, for simplicity, so that the ring of integers is really $\mathbb{Z}[\sqrt{D}]$, as earlier,

$$\mathfrak{O}/p\mathfrak{O} \;=\; \mathbb{Z}[x]/\langle p,\, x^2 - D\rangle \;=\; \mathbb{F}_p[x]/\langle x^2 - D\rangle$$

In $\mathbb{Q}(\omega)/\mathbb{Q}$ with ω an n^{th} root of unity, primes $p = 1 \bmod n$ *split completely*. As we will see, the integral closure $\mathfrak{O}$ of $\mathbb{Z}$ in $\mathbb{Q}(\omega)$ really is $\mathbb{Z}[\omega]$, and then, with Φ_n the n^{th} cyclotomic polynomial,

$$\mathfrak{O}/p\mathfrak{O} \;=\; \mathbb{Z}[x]/\langle p,\, \Phi_n\rangle \;=\; \mathbb{F}_p[x]/\langle \Phi_n\rangle$$

The n^{th} cyclotomic polynomial splits into linear factors over $\mathbb{F}_p$ exactly when $p = 1 \bmod n$, because $\mathbb{F}_p^\times$ is *cyclic*.

Proof that there are infinitely-many primes $p = 1 \bmod n$ is much easier than the general case of Dirichlet's theorem:

Given a list $p_1, \ldots, p_\ell$ of primes, consider $N = \Phi_n(tp_1 \ldots p_\ell)$ for integers t at our disposal. The cyclotomic Φ_n has integer coefficients and constant coefficient ± 1, so N is not divisible by any p_j. For sufficiently large t, N cannot be ± 1, either. Thus, N has prime factors p other than p_j.

At the same time, $p|\Phi_n(j)$ for an integer j says that j is a primitive n^{th} root of unity mod p, so $p = 1 \bmod n$. ///

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 $G_{\mathfrak{P}} \subset \mathrm{Gal}(K/E)$. ///