More about primes lying over...

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

**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

\[
\begin{array}{c}
\mathcal{K} \subset \mathcal{O} \subset \mathcal{P} \\
\mathcal{G}_\mathcal{P} \\
\mathcal{K}^{\mathcal{P}} \subset \mathcal{O}^{\mathcal{P}} \subset \mathcal{Q} = \mathcal{P} \cap \mathcal{K}^{\mathcal{P}} \\
k \subset \mathcal{O} \subset \mathcal{P} \\
\mathcal{O}^{\mathcal{P}} / \mathcal{Q} \\
\mathcal{O} / \mathcal{P} = \tilde{\kappa} \\
\mathcal{O} / \mathcal{P} = \kappa
\end{array}
\]
So far, we know that in the Galois case $G$ is transitive on primes $\mathfrak{P}$ lying over $p$.

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 $\sigma / p \rightarrow \mathcal{O}^\mathfrak{P} / q$ 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

$$ q_\mathfrak{P} = K^\mathfrak{P} \cap \sigma \mathfrak{P} $$

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

Thus, given $x \in \mathfrak{O}_\mathfrak{p}$, Sun-Ze’s theorem gives $y \in \mathfrak{O}_\mathfrak{p}$ such that

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

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, $\sigma y = 1 \mod \mathfrak{p}$ 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 $\sigma y$ with $\sigma \not\in G_\mathfrak{p}$. Therefore,

$$N_{k/K_\mathfrak{p}} y = x \mod \mathfrak{p}$$

The norm is in $\mathfrak{o}$, and the congruence holds mod $q$ since $x \in \mathfrak{O}_\mathfrak{p}$. ///
Claim: \( \tilde{\kappa} = \mathcal{O}/\mathfrak{p} \) is normal over \( \kappa = \mathfrak{o}/\mathfrak{p} \), and \( G_{\mathfrak{p}} \) surjects to \( \text{Gal}(\tilde{\kappa}/\kappa) \).

Proof: Let \( \alpha \in \mathcal{O} \) generate a separable subextension \( (\mod \mathfrak{p}) \) of \( \tilde{\kappa} \) over \( \kappa \). The minimal polynomial of \( \alpha \) over \( k \) has coefficients in \( \mathfrak{o} \) because \( \alpha \) 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 \( \alpha_i \mod \mathfrak{p} \).

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

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

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 $\alpha$ 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 $\alpha$ over $k$, and $\bar{f}$ 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 $\bar{f}$. $\text{Gal}(K/k)$ is transitive on the $\alpha_i$, so is transitive on the $\bar{\alpha}_i$. This proves surjectivity.
The **inertia subgroup** is the kernel $I_\mathfrak{P}$ of $G_\mathfrak{P} \to \text{Gal}(\tilde{\kappa}/\kappa)$, 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 $p$ is **inert** in $K/k$ (or in $\mathcal{O}/\mathfrak{o}$) the degree of the residue field extension (for any prime lying over $p$) is equal to the global field extension degree: $[\tilde{\kappa} : \kappa] = [K : k]$.

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

**Proof:** Galois groups of finite extensions of finite fields are (separable and) cyclic. The degree equality requires that the map $G_\mathfrak{P} \to \text{Gal}(\tilde{\kappa}/\kappa)$ 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 $C(x)$ no prime stays prime, since the residue fields are all $C$, which is already algebraically closed.

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

The Galois group of a cyclotomic extension $Q(\omega)/Q$ with $\omega$ an $n^{th}$ root of unity is $(Z/n)^{\times}$, 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 \( \Phi_n \) 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 \textit{primitive root} (=generator) for \((\mathbb{Z}/n)^\times\).

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

But \textit{Dirichlet’s theorem} on primes in arithmetic progression is necessary to prove existence of \textit{primes} equal mod \( n \) to a primitive root.

\textit{Quadratic reciprocity} gives a congruence condition for quadratic extensions of \( \mathbb{Q} \), and Dirichlet’s theorem again gives \textit{existence}.
\( p \) splits completely in \( K \) when there are \([K : k]\) distinct primes lying over \( p \) in \( \mathcal{O} \).

**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 \( D = 2, 3 \) mod 4, for simplicity, so that the ring of integers is really \( \mathbb{Z}[\sqrt{D}] \), as earlier,

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

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

\[
\mathcal{O}/p\mathcal{O} = \mathbb{Z}[x]/\langle p, \Phi_n \rangle = \mathbb{F}_p[x]/\langle \Phi_n \rangle
\]
The $n^{th}$ cyclotomic polynomial splits into linear factors over $\mathbb{F}_p$ exactly when $p = 1 \mod n$, because $\mathbb{F}_p^\times$ is cyclic.

Proof that there are infinitely-many primes $p = 1 \mod n$ 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 $\Phi_n$ has integer coefficients and constant coefficient $\pm 1$, so $N$ is not divisible by any $p_j$. For sufficiently large $t$, $N$ cannot be $\pm 1$, 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 $p = 1 \mod n$.  

///
**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 $q = \mathfrak{p} \cap K^\mathfrak{P}$. 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 $\mathfrak{p}$ 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 $\text{Gal}(E/k)$ is trivial. That is, the restriction of $G_{\mathfrak{P}}$ to $E$ is trivial, so $G_{\mathfrak{P}} \subset \text{Gal}(K/E)$. 

//

//