Math 129: Algebraic Number Theory
Lecture 12: Galois Extensions

William Stein

Thursday, March 15, 2004

1 Galois Extensions

Suppose $K \subset \mathbf{C}$ is a number field. Then K is *Galois* if every field homomorphism $K \to \mathbf{C}$ has image K, or equivalently, $\# \operatorname{Aut}(K) = [K : \mathbf{Q}]$. More generally, we have the following definition.

Definition 1.1 (Galois). An extension K/L of number fields is *Galois* if $\# \operatorname{Aut}(K/L) = [K : L]$, where $\operatorname{Aut}(K/L)$ is the group of automorphisms of K that fix L. We write $\operatorname{Gal}(K/L) = \operatorname{Aut}(K/L)$.

For example, $\mathbf{Q}$ is Galois (over itself), any quadratic extension K/L is Galois, since it is of the form $L(\sqrt{a})$, for some $a \in L$, and the nontrivial embedding is induced by $\sqrt{a} \mapsto -\sqrt{a}$, so there is always one nontrivial automorphism. If $f \in L[x]$ is an irreducible cubic polynomial, and a is a root of f, then one proves in a course in Galois theory that $L(a)$ is Galois over L if and only if the discriminant of f is a perfect square in L. Random number fields of degree bigger than 2 are rarely Galois (I will not justify this claim further in this course).

If $K/\mathbf{Q}$ is a number field, then the Galois closure K^{gc} of K is the field generated by all images of K under all embeddings in $\mathbf{C}$ (more generally, if K/L is an extension, the Galois closure of K over L is the field generated by images of embeddings $K \to \mathbf{C}$ that are the identity map on L). If $K = \mathbf{Q}(a)$, then K^{gc} is generated by each of the conjugates of a, and is hence Galois over $\mathbf{Q}$, since the image under an embedding of any polynomial in the conjugates of a is again a polynomial in conjugates of a.

How much bigger can the degree of K^{gc} be as compared to the degree of $K = \mathbf{Q}(a)$? There is a natural embedding of $\operatorname{Gal}(K^{\mathrm{gc}}/\mathbf{Q})$ into the group of permutations of the conjugates of a. If there are n conjugates of a, then this is an embedding $\operatorname{Gal}(K^{\mathrm{gc}}/\mathbf{Q}) \hookrightarrow S_n$, where S_n is the symmetric group on n symbols, which has order $n!$. Thus the degree of the K^{gc} over $\mathbf{Q}$ is a divisor of $n!$. Also the Galois group is a transitive subgroup of S_n, which constrains the possibilities further. When $n = 2$, we recover the fact that quadratic extensions are Galois. When $n = 3$, we see that the Galois closure of a cubic extension is either the cubic extension or a quadratic extension of the cubic extension. It turns out that that Galois closure of a cubic extension is obtained by adjoining the square root of the discriminant. For an extension K of degree 5, it is "frequently" the case that the Galois closure has degree 120, and in fact it is a difficult and interesting problem to find examples of degree 5 extension in which the Galois closure has degree smaller than 120 (according to MAGMA: the only possibilities for the order of a transitive proper subgroup of S_5 are 5, 10, 20, and 60; there are five transitive subgroups of S_5 out of the total of 19 subgroups of S_5).

Let n be a positive integer. Consider the field $K = \mathbf{Q}(\zeta_n)$, where $\zeta_n = e^{2\pi i/n}$ is a primitive nth root of unity. If $\sigma : K \to \mathbf{C}$ is an embedding, then $\sigma(\zeta_n)$ is also an nth root of unity, and the group of nth roots of unity is cyclic, so $\sigma(\zeta_n) = \zeta_n^m$ for some m which is invertible modulo n. Thus K is Galois and $\mathrm{Gal}(K/\mathbf{Q}) \hookrightarrow (\mathbf{Z}/n\mathbf{Z})^*$. However, $[K : \mathbf{Q}] = n$, so this map is an isomorphism. (Side note: Taking a p-adic limit and using the maps $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Gal}(\mathbf{Q}(\zeta_{p^r})/\mathbf{Q})$, we obtain a homomorphism $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{Z}_p^*$, which is called the p-adic cyclotomic character.)

Compositums of Galois extensions are Galois. For example, the biquadratic field $K = \mathbf{Q}(\sqrt{5}, \sqrt{-1})$ is a Galois extension of $\mathbf{Q}$ of degree 4.

Fix a number field K that is Galois over a subfield L. Then the Galois group $G = \mathrm{Gal}(K/L)$ acts on many of the object that we have associated to K, including:

- the integers $\mathcal{O}_K$,
- the units U_K,
- the group of nonzero fractional ideals of $\mathcal{O}_K$,
- the class group $\mathrm{Cl}(K)$, and
- the set $S_\mathfrak{p}$ of prime ideals $\mathfrak{P}$ lying over a given prime $\mathfrak{p}$ of $\mathcal{O}_L$.

In the next section we will be concerned with the action of $\mathrm{Gal}(K/L)$ on $S_\mathfrak{p}$, though actions on each of the other objects, especially $\mathrm{Cl}(K)$, will be of further interest.

2 Decomposition of Primes

Fix a prime $\mathfrak{p} \subset \mathcal{O}_K$ and write $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$, so $S_\mathfrak{p} = \{\mathfrak{P}_1, \ldots, \mathfrak{P}_g\}$.

Definition 2.1 (Residue class degree). Suppose $\mathfrak{P}$ is a prime of $\mathcal{O}_K$ lying over $\mathfrak{p}$. Then the *residue class degree* of $\mathfrak{P}$ is

$$f_{\mathfrak{P}/\mathfrak{p}} = [\mathcal{O}_K/\mathfrak{P} : \mathcal{O}_L/\mathfrak{p}],$$

i.e., the degree of the extension of residue class fields.

If $M/K/L$ is a tower of field extensions and $\mathfrak{q}$ is a prime of M over $\mathfrak{P}$, then

$$f_{\mathfrak{q}/\mathfrak{p}} = [\mathcal{O}_M/\mathfrak{q} : \mathcal{O}_L/\mathfrak{p}] = [\mathcal{O}_M/\mathfrak{q} : \mathcal{O}_K/\mathfrak{P}] \cdot [\mathcal{O}_K/\mathfrak{P} : \mathcal{O}_L/\mathfrak{p}] = f_{\mathfrak{q}/\mathfrak{P}} \cdot f_{\mathfrak{P}/\mathfrak{p}},$$

so the residue class degree is multiplicative in towers.

Note that if $\sigma \in \mathrm{Gal}(K/L)$ and $\mathfrak{P} \in S_p$, then σ induces an isomorphism of finite fields $\mathcal{O}_K/\mathfrak{P} \to \mathcal{O}_K/\sigma(\mathfrak{P})$ that fixes the common subfield $\mathcal{O}_L/\mathfrak{p}$. Thus the residue class degrees of $\mathfrak{P}$ and $\sigma(\mathfrak{P})$ are the same. In fact, much more is true.

Theorem 2.2. *Suppose K/L is a Galois extension of number fields, and let $\mathfrak{p}$ be a prime of $\mathcal{O}_L$. Write $\mathfrak{p}\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$, and let $f_i = f_{\mathfrak{P}_i/\mathfrak{p}}$. Then $G = \mathrm{Gal}(K/L)$ acts transitively on the set $S_\mathfrak{p}$ of primes $\mathfrak{P}_i$,*

$$e_1 = \cdots = e_g, \qquad f_1 = \cdots = f_g,$$

and $efg = [K : L]$, where e is the common value of the e_i and f is the common value of the f_i.

Proof. For simplicity, we will give the proof only in the case $L = \mathbf{Q}$, but the proof works in general. Suppose $p \in \mathbf{Z}$ and $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$, and $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_g\}$. We will first prove that G acts transitively on S. Let $\mathfrak{p} = \mathfrak{p}_i$ for some i. Recall that we proved long ago, using the Chinese Remainder Theorem, that there exists $a \in \mathfrak{p}$ such that $(a)/\mathfrak{p}$ is an integral ideal that is coprime to $p\mathcal{O}_K$. The product

$$I = \prod_{\sigma \in G} \sigma((a)/\mathfrak{p}) = \prod_{\sigma \in G} \frac{(\sigma(a))\mathcal{O}_K}{\sigma(\mathfrak{p})} = \frac{(\mathrm{Norm}_{K/\mathbf{Q}}(a))\mathcal{O}_K}{\displaystyle\prod_{\sigma \in G} \sigma(\mathfrak{p})} \tag{2.1}$$

is a nonzero integral $\mathcal{O}_K$ ideal since it is a product of nonzero integral $\mathcal{O}_K$ ideals. Since $a \in \mathfrak{p}$ we have that $\mathrm{Norm}_{K/\mathbf{Q}}(a) \in \mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}$. Thus the numerator of the rightmost expression in (2.1) is divisible by $p\mathcal{O}_K$. Also, because $(a)/\mathfrak{p}$ is coprime to $p\mathcal{O}_K$, each $\sigma((a)/\mathfrak{p})$ is coprime to $p\mathcal{O}_K$ as well. Thus I is coprime to $p\mathcal{O}_K$. Thus the denominator of the rightmost expression in (2.1) must also be divisibly by $p\mathcal{O}_K$ in order to cancel the $p\mathcal{O}_K$ in the numerator. Thus for any i we have

$$\prod_{j=1}^{g} \mathfrak{p}_j^{e_j} = p\mathcal{O}_K \;\Big|\; \prod_{\sigma \in G} \sigma(\mathfrak{p}_i),$$

which in particular implies that G acts transitively on the $\mathfrak{p}_i$.

Choose some j and suppose that $k \neq j$ is another index. Because G acts transitively, there exists $\sigma \in G$ such that $\sigma(\mathfrak{p}_k) = \mathfrak{p}_j$. Applying σ to the factorization $p\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}$, we see that

$$\prod_{i=1}^{g} \mathfrak{p}_i^{e_i} = \prod_{i=1}^{g} \sigma(\mathfrak{p}_i)^{e_i}.$$

Taking $\mathrm{ord}_{\mathfrak{p}_j}$ on both sides we get $e_j = e_k$. Thus $e_1 = e_2 = \cdots = e_g$.

As was mentioned right before the statement of the theorem, for any $\sigma \in G$ we have $\mathcal{O}_K/\mathfrak{p}_i \cong \mathcal{O}_K/\sigma(\mathfrak{p}_i)$, so by transitivity $f_1 = f_2 = \cdots = f_g$. Since $\mathcal{O}_K$ is a lattice in K, we have

$$\begin{aligned}[K : \mathbf{Q}] &= \dim_{\mathbf{Z}} \mathcal{O}_K = \dim_{\mathbf{F}_p} \mathcal{O}_K/p\mathcal{O}_K \\ &= \dim_{\mathbf{F}_p} \left(\bigoplus_{i=1}^{g} \mathcal{O}_K/\mathfrak{p}_i^{e_i} \right) = \sum_{i=1}^{g} \mathrm{Norm}_{K/\mathbf{Q}}(\mathfrak{p}_i^{e_i}) = \sum_{i=1}^{g} e_i f_i = efg,\end{aligned}$$

which completes the proof. □

The rest of this section illustrates the theorem for quadratic fields and a cubic field and its Galois closure.

2.1 Quadratic Extensions

Suppose $K/\mathbf{Q}$ is a quadratic field. Then K is Galois, so for each prime $p \in \mathbf{Z}$ we have $2 = efg$. There are exactly three possibilties:

- **Ramified:** $e = 2$, $f = g = 1$: The prime p ramifies in $\mathcal{O}_K$, so $p\mathcal{O}_K = \mathfrak{p}^2$. There are only finitely many such primes, since if $f(x)$ is the minimal polynomial of a generator for $\mathcal{O}_K$, then p ramifies if and only if $f(x)$ has a multiple root modulo p. However, $f(x)$ has a multiple root modulo p if and only if p divides the discriminant of $f(x)$, which is nonzero because $f(x)$ is irreducible over $\mathbf{Z}$. (This argument shows there are only finitely many ramified primes in any number field. In fact, we will later show that the ramified primes are exactly the ones that divide the discriminant.)

- **Inert:** $e = 1$, $f = 2$, $g = 1$: The prime p is inert in $\mathcal{O}_K$, so $p\mathcal{O}_K = \mathfrak{p}$ is prime. This happens 50% of the time, which is suggested by quadratic reciprocity (but not proved this way), as we will see illustrated below for a particular example.

- **Split:** $e = f = 1$, $g = 2$: The prime p splits in $\mathcal{O}_K$, in the sense that $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ with $\mathfrak{p}_1 \neq \mathfrak{p}_2$. This happens the other 50% of the time.

Suppose, in particular, that $K = \mathbf{Q}(\sqrt{5})$, so $\mathcal{O}_K = \mathbf{Z}[\gamma]$, where $\gamma = (1+\sqrt{5})/2$. Then $p = 5$ is ramified, since $p\mathcal{O}_K = (\sqrt{5})^2$. More generally, the order $\mathbf{Z}[\sqrt{5}]$ has index 2 in $\mathcal{O}_K$, so for any prime $p \neq 2$ we can determine the factorization of p in $\mathcal{O}_K$ by finding the factorization of the polynomial $x^2 - 5 \in \mathbf{F}_p[x]$. The polynomial $x^2 - 5$ splits as a product of two distinct factors in $\mathbf{F}_p[x]$ if and only if $e = f = 1$ and $g = 2$. For $p \neq 2, 5$ this is the case if and only if 5 is a square in $\mathbf{F}_p$, i.e., if $\left(\frac{5}{p}\right) = 1$, where $\left(\frac{5}{p}\right)$ is $+1$ if 5 is a square mod p and -1 if 5 is not. By quadratic reciprocity,

$$\left(\frac{5}{p}\right) = (-1)^{\frac{5-1}{2}\cdot\frac{p-1}{2}} \cdot \left(\frac{p}{5}\right) = \left(\frac{p}{5}\right) = \begin{cases} +1 & \text{if } p \equiv \pm 1 \pmod 5 \\ -1 & \text{if } p \equiv \pm 2 \pmod 5). \end{cases}$$

Thus whether p splits or is inert in $\mathcal{O}_K$ is determined by the residue class of p modulo 5.

2.2 The Cube Roots of Two

Suppose $K/\mathbf{Q}$ is not Galois. Then e_i, f_i, and g are defined for each prime $p \in \mathbf{Z}$, but we need not have $e_1 = \cdots = e_g$ or $f_1 = \cdots = f_g$. We do still have that $\sum_{i=1}^{g} e_i f_i = n$, by the Chinese Remainder Theorem.

For example, let $K = \mathbf{Q}(\sqrt[3]{2})$. We know that $\mathcal{O}_K = \mathbf{Z}[\sqrt[3]{2}]$. Thus $2\mathcal{O}_K = (\sqrt[3]{2})^3$, so for 2 we have $e = 3$ and $f = g = 1$. To factor $3\mathcal{O}_K$, we note that working modulo 3 we have

$$x^3 - 2 = (x-2)(x^2+2x+1) = (x+1)(x+1)^2 = (x+1)^3 \in \mathbf{F}_3[x],$$

so

$$3\mathcal{O}_K = (3, \sqrt[3]{2}+1)^3.$$

Thus $e_1 = 3$, $f_1 = 1$, and $g = 1$. Next, working modulo 5 we have

$$x^3 - 2 = (x+2)(x^2+3x+4) \in \mathbf{F}_5[x],$$

and the quadratic factor is irreducible. Thus

$$5\mathcal{O}_K = (5, \sqrt[3]{2}+2)\cdot(5, \sqrt[3]{2}^2 + 3\sqrt[3]{2}+4).$$

Thus here $e_1 = e_2 = 1$, $f_1 = 1$, $f_2 = 2$, and $g = 2$.

3 The Decomposition and Inertia Groups

Fix a finite Galois extension $K/\mathbf{Q}$ with Galois group $G = \mathrm{Gal}(K/\mathbf{Q})$. Let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime lying over a prime $p \in \mathbf{Z}$.

Definition 3.1 (Decomposition Group). The *Decomposition group* of $\mathfrak{p}$ is

$$D_{\mathfrak{p}} = \{\sigma \in G : \sigma(\mathfrak{p}) = \mathfrak{p}\} \subset G.$$

Remark 3.2. Note that $D_{\mathfrak{p}}$ is called the "splitting group" in [Swinnerton-Dyer], but everybody I know now calls it the decomposition group, so that is what we'll call it.

Let $\mathbf{F}_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$ denote the residue class field of $\mathfrak{p}$. In this section we will prove that there is a natural exact sequence

$$1 \to I_\mathfrak{p} \to D_\mathfrak{p} \to \mathrm{Gal}(\mathbf{F}_\mathfrak{p}/\mathbf{F}_p) \to 1,$$

where $I_\mathfrak{p}$ is the *inertia subgroup* of $D_\mathfrak{p}$, and $\#I_\mathfrak{p} = e$. The most interesting part of the proof is showing that the natural map $D_\mathfrak{p} \to \mathrm{Gal}(\mathbf{F}_\mathfrak{p}/\mathbf{F}_p)$ is surjective.

We will also discuss the structure of $D_\mathfrak{p}$ and introduce Frobenius elements, which play a crucial roll in understanding Galois representations.