On the automorphism group of algebraic number fields

Minhyong Kim

Given a field F, we denote by $\mathrm{Aut}(F)$ the group of field automorphisms of F. Recall that an *algebraic number field* is a finite extension of $\mathbb{Q}$.

We wish to prove

For most algebraic number fields F, we have

$$Aut(F) = \{1\}.$$

The statement here is not precise, and we will not bother to make it so. However, recall that any algebraic number field F has a primitive element α, so that $F = \mathbb{Q}(\alpha)$. If $f(x) \in \mathbb{Q}[x]$ is the irreducible polynomial of α, then

$$F \simeq \mathbb{Q}[x]/(f(x)).$$

For any polynomial f, denote by $\mathbb{Q}(f)$ the splitting field of f and

$$G_f := \mathrm{Gal}(\mathbb{Q}(f)/\mathbb{Q}) = \mathrm{Aut}(\mathbb{Q}(f)).$$

(We will diverge here a bit from the notation in the textbook, and write $\mathrm{Gal}(K/F)$ for the field automorphisms of K that act trivially on F.) What we will actually show is this:

Proposition 0.1. *Let $f \in \mathbb{Q}[x]$ be a polynomial of degree $n \geq 3$. Suppose $G_f \simeq S_n$. Then $Aut(\mathbb{Q}[x]/(f(x))) = \{1\}$.*

It is a fact, which we will not prove here, that f satisfying $G_f \simeq S_n$ is of density 1 among all polynomials of degree n, giving a precise mathematical interpretation of the original statement.

Lemma 0.2. *Let K/F be a Galois extension and suppose K' is an extension field of K (and hence, of F). Then for any embedding*

$$\tau : K \hookrightarrow K',$$

we have $\tau(K) = K$.

That is, any embedding τ is induces an automorphism of K. Notice that for a field like $\mathbb{Q}(2^{1/3}) \subset \mathbb{C}$, there is an embedding

$$\tau : \mathbb{Q}(2^{1/3}) \hookrightarrow \mathbb{C}$$

that takes $2^{1/3}$ to $\zeta_3 2^{1/3}$. This embedding will have an image different from $\mathbb{Q}(2^{1/3})$. This of course is because $\mathbb{Q}(2^{1/3})/\mathbb{Q}$ is not Galois. For $K \subset \mathbb{C}$ that is a Galois extension of $\mathbb{Q}$, the lemma says that any complex embedding will have the same image K. The proof of the lemma is easy and details are left to the reader. The idea is that $K = F(\alpha)$ for a primitive element α with irreducible polynomial $f(x) \in F[x]$. Then any embedding τ will have to take α to a root of $f(x)$. But since K/F is Galois, all the roots of f are in K.

Lemma 0.3. *Let K/F be Galois and let L be an intermediate field: $F \subset L \subset K$. Then any automorphism $\sigma \in Gal(L/F)$ extends to an automorphism*

$$\tau \in Gal(K/F).$$

Proof. We have $K = L(\alpha)$ for an element α with irreducible polynomial $f(x) \in L[x]$. Write $\sigma(f) \in L[x]$ for the polynomial obtained by applying σ to the coefficients of f. Let $K' \supset K$ be an extension field in which $\sigma(f)$ has a root β. Then we have an isomorphism

$$\tau : K \simeq L[x]/(f(x)) \simeq L[x]/(\sigma(f(x)) \simeq L(\beta) \subset K'.$$

By the previous lemma, $\tau(K) = K$, so τ gives rise to an automorphism of K. The second isomorphism restricts to σ on L while the others are the identity on L, so τ extends σ. $\square$

Lemma 0.4. *Let K/F be Galois and let L be an intermediate field: $F \subset L \subset K$. Let $H = Gal(K/L)$ so that L is the fixed field of H. Then there is an isomorphism*

$$N(H)/H \simeq Gal(L/F),$$

where $N(H)$ denotes the normalizer of H inside $Gal(K/F)$.

Of course, when $H < \mathrm{Gal}(K/F)$ is normal, this becomes the statement:

$$\mathrm{Gal}(K/F)/\mathrm{Gal}(K/L) \simeq \mathrm{Gal}(L/F)$$

proved in an earlier lecture.

Proof. First, let $\tau \in N(H)$. Then for any $x \in L$ and $h \in H$, we have

$$h\tau(x) = \tau(\tau^{-1}h\tau)x = \tau x$$

since $\tau^{-1}h\tau \in H$. So $\tau(x)$ is fixed by all elements of H. Hence, $\tau(x) \in L$. Therefore, the restriction

$$\tau \mapsto \tau|L$$

induces a homomorphism $N(H) \to \mathrm{Gal}(L/F)$, whose kernel is exactly H. Thus, we have an injection

$$N(H)/H \hookrightarrow \mathrm{Gal}(L/F).$$

On the other hand, any $\sigma \in \mathrm{Gal}(L/F)$ extends to an automorphism τ of K. For this extension, we have $\tau(L) = L$, so $\tau^{-1}(L) = \tau^{-1}(\tau(L)) = L$. Thus, for any $h \in H$ and $x \in L$, we have $\tau^{-1}(x) \in L$, so that

$$\tau h \tau^{-1}(x) = \tau\tau^{-1}(x) = x.$$

That is, $\tau h \tau^{-1} \in H$, whereby $\tau \in N(H)$. Therefore, the restriction map $N(H) \to \mathrm{Gal}(L/F)$ is surjective, giving us the desired isomorphism

$$N(H)/H \simeq \mathrm{Gal}(L/F).$$

$\square$

Given H, it could very well be that $N(H)$ is not much bigger than H, so that $N(H)/H$ is quite small. It turns out our proposition is concerned exactly with a situation of this sort.

Proof of proposition. Let $\mathbb{Q}(f) \subset \mathbb{C}$ be the splitting field of f, so that

$$\mathbb{Q}(f) = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n),$$

where the α_i are the distinct roots of f. Then

$$\mathbb{Q}[x]/(f(x)) \simeq \mathbb{Q}(\alpha_n),$$

so we need only prove that $\mathrm{Aut}(\mathbb{Q}(\alpha_n)) = \{1\}$. If we use the given ordering of the roots to idenitfy G_f with S_n, then we can ask for the subgroup corresponding to the subfield

$$\mathbb{Q}(\alpha_n) \subset \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

These are the automorphisms that fix α_n, and hence, can exactly be identified with $S_{n-1} \subset S_n$. Therefore, we have

$$\mathrm{Aut}(\mathbb{Q}(\alpha_n)) \simeq N(S_{n-1})/S_{n-1},$$

where the normalizer is taken inside S_n. So the proposition follows from the simple observation that

If $n \geq 3$, then $N(S_{n-1}) = S_{n-1}$.

To see this, let $\sigma \in S_n$ normalize S_{n-1}, let $i \in \{1, \ldots, n-1\}$, and $j = \sigma(i)$. Choose $k \neq i$ in $\{1, \ldots, n-1\}$. (This is possible since $n \geq 3$.) Then the transposition $(i\ k)$ is not the identity. Under conjugation, we have

$$\sigma(i\ k)\sigma^{-1} = (j\ \sigma(k)) \in S_{n-1}.$$

But this implies $j \in \{1, \ldots, n-1\}$. Therefore, σ stabilizes the set $\{1, \ldots, n-1\}$, implying that $\sigma(n) = n$, and hence, $\sigma \in S_{n-1}$.

□