CONSTRUCTIBILITY AND GALOIS THEORY

1. Constructibility

Identify the plane with $\mathbb{C}$. The set $\mathcal{C} \subseteq \mathbb{C}$ of **constructible numbers** is the collection of numbers which can be realized, starting from 0 and 1, and applying a finite sequence of the following operations:

(A1) Draw a line through two points which have already been constructed.

(A2) Draw a circle with the center at a point that has already been constructed, and the circumference passing through another point that has been constructed.

(A3) Add to the collection of constructed points an intersection point of two non-parallel lines, two circles, or a line and a circle.

An angle θ is a **constructible angle** if it is possible, starting from 0 and 1 and using a finite sequence of the above operations, to construct two lines whose intersection forms the angle θ. The collection of all constructible angles is denoted by Θ. The set $\mathcal{C}$ is completely characterized by the following result.

Theorem 1. *The set $\mathcal{C}$ is a subfield of $\mathbb{C}$. A complex number α lies in $\mathcal{C}$ if and only if there exists an integer $n \geq 0$ and a sequence of fields $K_0, K_1, \ldots, K_n \subseteq \mathbb{C}$ satisfying:*

(i) $K_0 = \mathbb{Q}$ *and* $K_n = \mathbb{Q}(\alpha)$,
(ii) $K_{i-1} \subseteq K_i$, *for each* $1 \leq i \leq n$, *and*
(iii) $[K_i : K_{i-1}] = 2$ *for each* $1 \leq i \leq n$.

2. Galois Theory

If K is a field then an isomorphism from K to itself is called an **automorphism** of K. The collection of all automorphisms of K is denoted by $\mathrm{Aut}(K)$. An element $\sigma \in \mathrm{Aut}(K)$ **fixes** a subset $A \subseteq K$ if $\sigma a = a$ for every $a \in A$. If K/F is a field extension the the collection of automorphisms of K which fix F is denoted $\mathrm{Aut}(K/F)$.

The set $\mathrm{Aut}(K)$ forms a group under composition of maps, and $\mathrm{Aut}(K/F)$ forms a subgroup. For any subgroup $H \leqslant \mathrm{Aut}(K)$, the collection of elements fixed by H, denoted K_H, is a subfield of K, called the **fixed field** of H.

For any field K, the **prime subfield** of K is the smallest field contained in K. If $\mathrm{char}(K) = 0$ then the prime subfield of K is isomorphic to $\mathbb{Q}$. If $\mathrm{char}(K) = p$

for some prime p then the prime subfield of K is isomorphic to $\mathbb{F}_p$. It is not difficult to show that every element of $\mathrm{Aut}(K)$ fixes the prime subfield of K.

Suppose that K/F is a field extension and that $\alpha \in K$ is algebraic over F. Let f_α be the minimal polynomial for α over F. Then it is an important fact (which you should know how to prove) that, for any $\sigma \in \mathrm{Aut}(K/F)$, we have that $f_\alpha(\sigma(\alpha)) = 0$. In other words, elements of $\mathrm{Aut}(K/F)$ always send α to another root of f_α.

In trying to understand the group $\mathrm{Aut}(K/F)$, it is often useful to combine the above observation with the following fact: If K/F is given by $K = F(\alpha_1, \ldots, \alpha_n)$, then every element $\sigma \in \mathrm{Aut}(K/F)$ is uniquely determined by the values of $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$. This shows, in particular, that if K/F is a finite extension then $|\mathrm{Aut}(K/F)| < \infty$. In fact, we can say more.

Theorem 2. *If K/F is any finite extension then*

$$|\mathrm{Aut}(K/F)| \leq [K : F],$$

with equality if and only if F is the fixed field of $\mathrm{Aut}(K/F)$*.*

A finite extension K/F is called a **Galois extension** if $|\mathrm{Aut}(K/F)|$ is equal to $[K : F]$. In this case, $\mathrm{Aut}(K/F)$ is also called the **Galois group** of K/F, and denoted by $\mathrm{Gal}(K/F)$. The theorem above gives one characterization of Galois extensions. Another characterization is the following.

Theorem 3. *A finite extension K/F is Galois if and only if K is the splitting field of a separable polynomial with coefficients in F. Furthermore, if K/F is Galois then it is separable and every irreducible polynomial in $F[x]$ which has a root in K, splits completely.*

Now we present the main theorem of the course, which establishes an explicit bijection between subgroups of the Galois group of a Galois extension, and intermediate fields of the extension.

Theorem 4 (Fundamental Theorem of Galois Theory). *If K/F is a Galois extension, with Galois group G, then:*

(i) *There is a bijection between subgroups H of G and intermediate fields of the extension K/F, given by the map $H \mapsto K_H$. Furthermore, $[K : K_H] = |H|$ (equivalently, $[K_H : F] = |G : H|$).*

(ii) *For each $H \leqslant G$, the extension K_H/F is Galois if and only if H is normal in G. If K_H/F is Galois then* $\mathrm{Gal}(K_H/F) \cong G/H$*.*