

# Math 250A Lecture 21 Notes

Daniel Raban

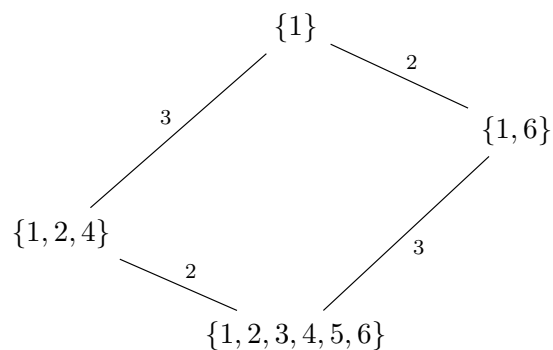
November 9, 2017

## 1 The Fundamental Theorem of Galois Theory

### 1.1 Proof and an example

Here is the example of the fundamental theorem that we started last time:

**Example 1.1.** Last time we had  $L = \mathbb{Q}[\zeta]$ , where  $\zeta = e^{2\pi i/7}$ . We wanted to find all subfields of  $L$ . This had the Galois group  $(\mathbb{Z}/7\mathbb{Z})^*$ , which has subgroups



We should have 2 intermediate fields between  $\mathbb{Q}$  and  $\mathbb{Q}(\zeta)$ , of degree 2 and 3. What are they?

Let's find the degree 2 field. The elements are fixed by  $H = \{1, 2, 4\}$ . One fixed element is  $a = \zeta + \zeta^2 + \zeta^4$ , which is not in  $\mathbb{Q}$ . What is  $a$ ? We must find a quadratic equation with root  $a$ .

$$a^2 = \zeta + \zeta^2 + 2\zeta^3 + \zeta^4 + 2\zeta^5 + 2\zeta^6$$
$$a^2 + a = 2)\zeta + \zeta^2 + \dots + \zeta^6$$

So  $a^2 + a + 2 = 0$ , which makes  $a = \frac{-1+\sqrt{-7}}{2}$ . So the degree 2 field is  $\mathbb{Q}[a] = \mathbb{Q}[\sqrt{-7}]$ .

Let's find the degree 3 subfield. Let  $J = \{1, 6\}$ . Look for an invariant element; we choose  $\zeta + \zeta^6 = \zeta + \zeta^{-1}$ . Note that  $\zeta = e^{2\pi i/7} = \cos(2\pi/7) + i \sin(2\pi/7)$ . So  $\zeta + \zeta^{-1} = 2 \cos(2\pi/7)$ .

Alternatively, we can find the irreducible equation it satisfies. We have

$$(\zeta + \zeta^{-1})^3 = \zeta^3 + 3\zeta + 3\zeta^{-1} + \zeta^{-3}.$$

$$(\zeta + \zeta^{-1})^2 = \zeta^2 + 2 + \zeta^{-2}.$$

Since  $\zeta^3 + \zeta^2 + \zeta + \dots + \zeta^{-3} = 0$ , we have that  $\zeta - \zeta^{-1}$  is a root of  $x^3 + x^2 - 2x - 1$ . The 3 roots of this polynomial are  $2 \cos(2\pi/7)$ ,  $2 \cos(4\pi/7)$ , and  $2 \cos(8\pi/7)$ .

**Theorem 1.1** (Fundamental theorem of Galois theory). *Let  $M/K$  be a Galois extension with Galois group  $G$ . Then there is a correspondence of subextensions  $L$  of  $M$  with subgroups  $H$  of  $G$  given by  $L \mapsto \text{Gal}(M/L)$ . and  $H \subseteq G \mapsto M^H$ . Moreover, these maps are inverses of each other.*

*Proof.* We want to show that  $L = M^{\text{Gal}(M/L)}$ . We have  $L \subseteq M^{\text{Gal}(M/L)}$ , so it is enough to show that they have the same size. We show that they have the same index in  $M$ .

Similarly, we have that  $H \subseteq \text{Gal}(M : M^H)$ , so to show that they are the same, it also suffices to show that they are the same size. So the theorem follows if we show:

1.  $|\text{Gal}(M : L)| = [M : L]$ .
2.  $[M : M^H] = |H|$ .

The key point is to recall our lemma from last lecture: if  $K \subseteq L$  and  $K \subseteq M$ , there are at most  $[L : K]$  maps  $L \rightarrow M$  extending the identity map of  $K$ .

To prove the first statement, observe that  $|\text{Gal}(M/L)| \leq [M : L]$  by the lemma. Now suppose it is strictly less. Look at  $K \subseteq L \subseteq M$ . By the multiplicativity of indices, there are  $< [L : K][M : L] = [M : K]$  maps from  $M \rightarrow M$ . But since  $M/K$  is Galois, there are exactly  $[M : K]$  maps  $M \rightarrow M$ , which is a contradiction.

The proof of the second statement is similar, and we leave it as an exercise. □

## 1.2 Applications of the fundamental theorem

### 1.2.1 Construction of a 17-sided regular polygon

We can use Galois theory to prove the existence of a construction of a 17-sided regular polygon using a ruler and compass.<sup>1</sup>

**Example 1.2.** We want to construct  $\zeta$ , where  $\zeta^{17} = 1$ . We have  $\frac{\zeta^{17}-1}{\zeta-1} = 0$ . Recall that this was an irreducible polynomial of degree 16. The idea is that we can find intermediate fields  $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\beta) \subseteq \mathbb{Q}(\gamma) \subseteq \mathbb{Q}(\zeta)$ . We can construct degree 2 extensions with a ruler and compass because we can construct square roots with a ruler and compass.

---

<sup>1</sup>Gauss became famous as a teenager by becoming the first to give an explicit construction.

Look at the Galois group  $(\mathbb{Z}/17\mathbb{Z})^* \cong \mathbb{Z}/16\mathbb{Z}$ . This has subgroups  $0 \subseteq \mathbb{Z}/2\mathbb{Z} \subseteq \mathbb{Z}/4\mathbb{Z} \subseteq \mathbb{Z}/8\mathbb{Z} \subseteq \mathbb{Z}/16\mathbb{Z}$ , so we can find the desired field extensions. If we want to find out what the fields are, we can proceed as earlier. Explicitly, the subgroups are

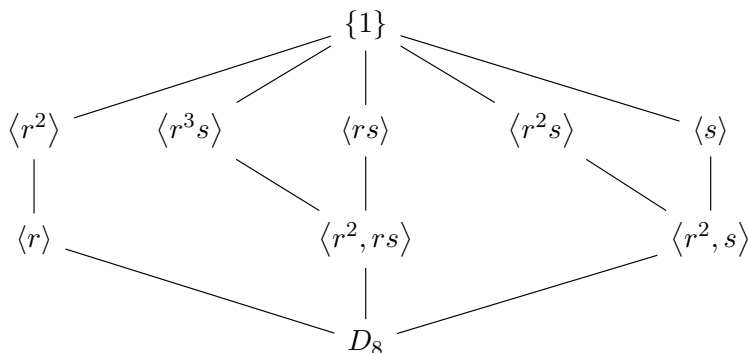
$$\{0\} \subseteq \{1, 16\} \subseteq \{1, 4, 13, 16\} \subseteq \{1, 2, 4, 8, 9, 13, 15, 16\} \subseteq \mathbb{Z}/16\mathbb{Z},$$

so we can find the fixed fields of these subgroups:

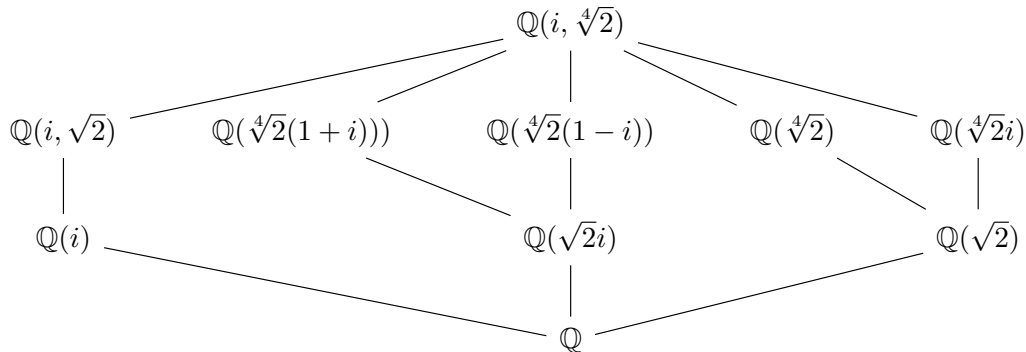
$$\mathbb{Q}(\zeta), \mathbb{Q}(\zeta + \zeta^{16}), \mathbb{Q}(\zeta + \zeta^4 + \zeta^{13} + \zeta^{16}), \mathbb{Q}(\zeta^1 + \zeta^2 + \zeta^4 + \dots).$$

### 1.2.2 Subextensions of a splitting field

**Example 1.3.** Let's find all the subextensions of  $x^4 - 2$  over  $\mathbb{Q}$ . This has the roots  $\sqrt[4]{2}$ ,  $\sqrt[4]{2}i$ ,  $-\sqrt[4]{2}$ , and  $-\sqrt[4]{2}i$ . We have that  $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$  and  $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})] = 2$ , so the splitting field has degree 8 over  $\mathbb{Q}$ . If we draw out the roots in the complex plane, we get the vertices of the square. So the Galois group is the group of symmetries of the square,  $D_8$ . Its subgroups are:



So the subextensions are:



### 1.3 Extensions corresponding to normal subgroups and factor groups

In the previous example, The 3 subgroups of order 4 and the first subgroup of order 2 are normal. The other four subgroups of order 2 come in conjugate pairs. We can see that the corresponding extensions are normal. This is true in general.

**Proposition 1.1.** *Let  $H \subseteq \text{Gal}(L/K)$ . Then  $H$  is normal iff  $L^K/K$  is a normal extension.*

*Proof.*  $H$  is normal iff all conjugates of  $H$  under  $G$  are the same as  $H$ .  $L^K/K$  is normal iff all conjugates of  $L^K$  under the Galois group are the same as  $L^K$ .  $\square$

Suppose  $L/K$  is a field extension corresponding to  $H$  and is normal. What is the Galois group of  $L/K$ ? A standard blunder is to think that it is  $H$ , which is actually  $\text{Gal}(M/L)$ . In fact,  $\text{Gal}(L/K) = G/H$ . If we have  $\text{Aut}(M) \rightarrow \text{Aut}(L)$ , the kernel is everything fixing all elements of  $L$ . This is  $H$ .

### 1.4 Finding extensions corresponding to a given group

**Proposition 1.2.** *Let  $G$  be a finite group. Then there is a Galois extension  $L/K$  with Galois group  $G$ .*

*Proof.* First take  $G = S_n$ , and let  $L = \mathbb{Q}(x_1, x_2, \dots, x_n)$ , all rational functions in  $n$  variables. Now let  $K = L^{S_n}$ , the symmetric rational functions. If  $G$  is any finite group acting on any field  $L$ , then  $L/L^G$  is Galois with group  $G$ . So  $L/L^{S_n}$  is a Galois extension with Galois group  $S_n$ . The same works for when  $G$  is a subgroup of  $S_n$ ;  $L/L^G$  has Galois group  $G$ . The result follows by Cayley's theorem, that any finite group is a subgroup of some permutation group.  $\square$

This is very hard if you want a specific field  $K$ . The following is still an open problem: "Given a finite group  $G$ , is there an extension of  $\mathbb{Q}$  with Galois group  $G$ ?"

**Example 1.4.** Let  $G = \mathbb{Z}/5\mathbb{Z}$  and let  $\zeta^{11} = 1$ . Notice that  $\mathbb{Q}[\zeta]$  has Galois groups  $\mathbb{Z}/11\mathbb{Z}^* \cong \mathbb{Z}/10\mathbb{Z}$ , which has the quotient,  $\mathbb{Z}/5\mathbb{Z}$ . Explicitly, if we take the field  $\mathbb{Q}(\zeta)^{\mathbb{Z}/2\mathbb{Z}}$ , then its Galois group is  $(\mathbb{Z}/10\mathbb{Z})/(\mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}/5\mathbb{Z}$ .

**Example 1.5.** Let's find an extension of  $\mathbb{Q}$  with Galois group  $S_5$  (order 120). We take the splitting field of  $x^5 - 4x + 2$ . This is irreducible by Eisenstein's criterion. If you look at the graph, it has exactly 3 real roots (and hence 2 complex roots). The Galois group is a subgroup of  $S_5$ , the permutations of the 5 roots. The Galois group contains a 5-cycle, say (1 2 3 4 5), so its order is divisible by 5. The Galois group also contains a transposition (complex conjugation). A 5 cycle and a transposition generate  $S_5$  (exercise). So the Galois group of this splitting field is  $S_5$ .

This example generalizes into the following result:

**Proposition 1.3.** *If  $p$  is prime, we can find an extension  $L/\mathbb{Q}$  with Galois group  $S_p$ .*

**Corollary 1.1.** *If  $G$  is finite, we can find extensions  $L/K$  of  $\mathbb{Q}$  with  $\text{Gal}(L/K) = G$ .*

*Proof.* Let  $L$  be the extension with  $\text{Gal}(L/\mathbb{Q}) = S_p$  for some large  $p$ . Take  $G \subseteq S_p$ , and let  $K = L^G$ . □