PMATH348 — Fields and Galois Theory

Classnotes for Winter 2019

by

Johnson Ng

BMath (Hons), Pure Mathematics major, Actuarial Science Minor

University of Waterloo

Table of Contents

List of Definitions

List of Theorems

List of Procedures

Preface

This is a 3 part course; it is separated into

1. **Sylow's Theorem**

   which is a leftover from group theory (PMATH 347). It has little to do with the rest of the course, but PMATH 347 was a course that is already content-rich to a point where Sylow's Theorem gets pushed into the later course that is this course.

2. **Field Theory**

   is a somewhat understood concept from ring theory, where we learned that it is a special case of a ring where all of its elements have an inverse.

3. **Galois Theory**

   is the beautiful theory from the French mathematican Évariste Galois that ties field theory back to group theory. This allows us to reduce certain field theory problems into group theory, which, in some sense, is easier and better understood.

Part I

Sylow's Theorem

1 Lecture 1 Jan 07th

1.1 Cauchy's Theorem

Recall Lagrange's Theorem.

Theorem 1 (Lagrange's Theorem)

If G is a finite group and H is a subgroup of G [1], then $|H| \mid |G|$ [2].

[1] I shall write this as $H \leq G$ from hereon.
[2] This just means $|H|$ divides $|G|$.

The full converse is not true.

Example 1.1.1

Let $G = A_4$, the **alternating group** of 4 elements. Then $|G| = 12$ [3]. We have that $6 \mid 12$. We shall show that G has no subgroup of order 6.

[3] Recall that the symmetric group of 4 elements S_4 has order $4! = 24$, and an alternating group has half of its elements.

Suppose to the contrary that $H \leq G$ such that $|H| = 6$. Let $a \in G$ such that $|a| = 3$ [4] There are 8 such elements in G [5]. Note that the **index**[6] of H, $|G : H|$, is $\frac{|G|}{|H|} = 2$.

[4] i.e. the order of a is 3. This is a **trick**.
[5] This shall be left as an exercise.

Exercise 1.1.1
Prove that there are 8 *elements in* G *that have order* 3.

[6] The index of a subgroup is the number of unique cosets generated by H.

Now consider the **cosets** H, aH and a^2H. Since $|G : H| = 2$, we must have either

- $aH = H \implies a \in H$;
- $aH = a^{-1}H \overset{\text{'multiply' } a^{-1}}{\implies} H = aH \implies a \in H$; or
- $a^2H = H \overset{\text{'multiply' } a}{\implies} H = aH \implies a \in H$.

Thus all 8 elements of order 3 are in H but $|H| = 6$, a contradiction. Therefore, no such subgroup (of order 6) exists.

Our goal now is to establish a partial converse of Lagrange's Theorem. To that end, we shall first lay down some definitions.

Definition 1 (p-Group)

Let p be prime. We say that a group G is a p-group if $|G| = p^k$ for some $k \in \mathbb{N}$. For $H \leq G$, we say that H is a p-subgroup of G if H is a p-group.

Definition 2 (Sylow p-Subgroup)

Let G be a group such that $|G| = p^n m$ for some $n, m \in \mathbb{N}$, such that $p \nmid m$. If $H \leq G$ with order p^n, we call H a Sylow p-subgroup.

Recall Cauchy's Theorem for abelian groups[7].

[7] In the course I was in, we were introduced only to the full theorem and actually went through this entire part. See notes on PMATH 347.

Theorem 2 (Cauchy's Theorem for Abelian Groups)

If G is a finite abelian group, and p is prime such that $p \mid |G|$, then $|G|$ has an element of order p.

Definition 3 (Stabilizers and Orbits)

Let G be a finite group which acts on a finite set X[8]*. For $x \in X$, the stabilizers of x is the set*

$$\text{stab}(x) := \{g \in G : gx = x\} \leq G.$$

The orbits of x is a set

$$\text{orb}(x) := \{gx : g \in G\}.$$

[8] Recall that a group action is a function $\cdot : G \times X \to X$ such that

1. $g(hx) = (gh)x$; and
2. $ex = x$.

Note 1.1.1

One can verify that the function $G/\operatorname{stab}(x) \to \operatorname{orb}(x)$ *such that*

$$g\operatorname{stab}(x) \mapsto gx$$

is a bijection.

Theorem 3 (Orbit-Stabilizer Theorem)

Let G *be a group acting on a set* X*, and for each* $x \in X$*,* $\operatorname{stab}(x)$ *and* $\operatorname{orb}(x)$ *are the stabilizers and orbits of* x*, respectively. Then*

$$|G| = |\operatorname{stab}(x)| \cdot |\operatorname{orb}(x)|.$$

Moreover, if $x, y \in X$*, then either* $\operatorname{orb}(x) \cap \operatorname{orb}(y) = \emptyset$ *or* $\operatorname{orb}(x) = \operatorname{orb}(y)$*.*

The theorem is actually equivalent to Proposition 45 in the notes for PMATH 347. However, feel free to...

Exercise 1.1.2

prove Theorem 3 as an exercise.

Consequently, we have that

$$|X| = \sum |\operatorname{orb}(a_i)|,$$

where a_i are the distinct orbit representatives. Letting

$$X_G := \{x \in X : gx = x, g \in G\},$$

we have...

Theorem 4 (Orbit Decomposition Theorem)

$$|X| = |X_G| + \sum_{a_i \notin X_G} |\operatorname{orb}(a_i)|.$$

---

2 Lecture 2 Jan 09th

2.1 Sylow Theory

From the Orbit Decomposition Theorem, one special case is when G acts on $X = G$ by conjugation.

Corollary 5 (Class Equation)

From Theorem 4, if $X = G$, we have

$$\begin{aligned} |G| &= |Z(G)| + \sum |\text{orb}(a_i)| \qquad \text{(non-central } \uparrow\text{)} \\ &= |Z(G)| + \sum [G : \text{stab}(a_i)] \text{ by } Orbit - Stabilizer \\ &= |Z(G)| + \sum [G : C(a_i)], \end{aligned}$$

*where $C(a_i)$ is called the **centralizers** of G.*

Theorem 6 (First Sylow Theorem)

Let G be a finite group, and let $p \mid |G|$ such that p is prime. Then G contains a Sylow p-subgroup.

Proof

We proceed by induction on the size of G. If $|G| = 2$, then $p = 2$, and so G is its own Sylow p-subgroup [1].

[1] A 2-cycle is a Sylow p-group.

Consider a finite group G with $|G| \geq 2$. Let p be a prime that divides $|G|$, and assume that the desired result holds for smaller groups.

Let $|G| = p^n m$, where $n, m \in \mathbb{N}$, and $p \nmid m$.

Case 1: $p \mid |Z(G)|$ By Theorem 2, $\exists a \in Z(G)$ such that $|a| = p$. Since $\langle a \rangle \subsetneq Z(G)$, we have that

$$\langle a \rangle \triangleleft G \text{ and } |\langle a \rangle| = p.$$

[2] Notice that the group $G/\langle a \rangle$ is a group that has a lower order than G, and so by IH, $\exists \overline{H} \leq G/\langle a \rangle$ such that $\overline{H}$ is a Sylow p-subgroup of $G/\langle a \rangle$. Note that if $n = 1$. then $\langle a \rangle$ itself is the Sylow p-subgroup. WMA $n > 1$. We have that $|H| = p^{n-1}$. By correspondence,

$$\overline{H} = H/\langle a \rangle,$$

where $H \leq G$. By comparing the orders, we have

$$p^{n-1} = \frac{|H|}{p} \implies |H| = p^n.$$

Therefore H is a Sylow p-subgroup of G.

Case 2: $p \nmid Z(G)$ By the class equation, notice that

$$p^n m = |G| = |Z(G)| + \sum [G : C(a_i)], \tag{2.1}$$

and the summation cannot be 0 or p would otherwise divide $Z(G)$. Since p divides the LHS of Equation (2.1) and not $|Z(G)|$, and the sum is nonzero, we must have that $\exists a_i \in G$ such that $p \nmid [G : C(a_i)]$, since only then would $p \mid |G|$ [3]. Since $p \mid |G|$ but not $|G : C(a_i)|$, it must be that $p^n \mid |C(a_i)|$ by Lagrange [4].

Note that we have $|C(a_i)| \leq |G|$. Thus by IH, $C(a_i)$ has a Sylow p-subgroup, which is also a Sylow p-subgroup of G. □

Corollary 7 (Cauchy's Theorem)

If p is prime and $p \mid |G|$, then G has an element of order p.

[2] This feels like a struck of genius. Let's break it down and find some way that makes it easier to remember. We want to find $H \leq G$ such that $|H| = p^n$. We have $|\langle a \rangle| = p$. We want to be able to use the **Correspondence Theorem**, so we should adjust our materials to fit that mold: since $|\langle a \rangle| = p$, notice that

$$\frac{|G|}{|\langle a \rangle|} = p^{n-1} m.$$

This is a smaller group than G, and so IH tells us that it has a Sylow p-subgroup, say $\overline{H}$. By the Correspondence Theorem, we may retrieve H.

[3] This is after having this term 'neutralizing' $|G|$ so that the entire RHS is also divisible by p. If p already divides everything, and does not divide $|Z(G)|$, then p would not divide $|Z(G)|$.

[4] Having $p^n \mid |C(a_i)|$ would cancel out all the p's in $|G|$, thus rendering p unable to divide $|G : C(a_i)|$.

Proof

WLOG, WMA $|G| = p^n m$, where $n, m \in \mathbb{N}$ and $p \nmid m$. By Theorem 6, $\exists H \leq G$ such that H is a Sylow p-subgroup. Take $a \in H \setminus \{e\}$. Then $|a| = p^k$ for some $k \leq n$.

Let $b = a^{p^{k-1}}$. Notice that $b \neq e$, or it would contradict the definition of an order (for a). Then $b^p = \left(a^{p^{k-1}}\right)^p = a^p = e$. Therefore $|b| = p$ and $b \in G$. □

Definition 4 (Normalizer)

Let G be a group, and $H \leq G$. The set

$$N_G(H) = \left\{ g \in G \;\middle|\; gHg^{-1} = H \right\}$$

*is called the **normalizer** of H in G.*

Exercise 2.1.1

Verify that $N_G(H)$ is the largest subgroup of G that contains H as a normal subgroup.

Proof

It is clear by definition of a normalizer that $H \triangleleft N_G(H)$.

Suppose there exists $N_G(H) < \tilde{H} \leq G$ such that $H \triangleleft \tilde{H}$. Let $h \in \tilde{H} \setminus N_G(H)$. But since $H \triangleleft \tilde{H}$, we have

$$hHh^{-1} = H,$$

which implies that $h \in N_G(H)$, a contradiction. Therefore $N_G(H)$ is the largest subgroup that contains H as a normal subgroup. □

Before proceeding with the Sylow's next theorem, we require two lemmas.

Lemma 8 (Intersection of a Sylow p-subgroup with any other p-subgroups)

Let G be a finite group and p a prime such that $p \mid |G|$. Let $P, Q \leq G$ be a Sylow p-subgroup and a (regular) p-subgroup, respectively. Then

$$Q \cap N_G(P) = Q \cap P. \tag{2.2}$$

Lemma 8 tells us that if we can find a p-subgroup Q of G, then the elements in Q that serves as the stabilizers of P are precisely the elements that Q shares with P. This is uninteresting if P is either abelian or normal, but it would highlight what $Z(P)$ is.

Proof

Since $P \subseteq N_G(P)$, $\subseteq$ of Equation (2.2) is done.

Let $N = N_G(P)$, and let $H = Q \cap N$. WTS $H \subseteq Q \cap P$. Since $H = Q \cap N \subseteq Q$, it suffices to show that $H \subseteq P$. Since P is a Sylow p-subgroup, let $|P| = p^n$. By Lagrange, we have that $|H| = p^m$ for some $m \leq n$. Since $P \triangleleft N$, we have that $HP \leq N$ [5]. Moreover, we have that

$$|HP| = \frac{|H|\,|P|}{|H \cap P|} = p^k$$

for some $k \leq n$. Also, $P \subset HP$, and so $n \leq k$, implying that $k = n$. Thus $P = HP$, and thus

$$H \subseteq HP = P,$$

as required. □

[5] See PMATH 347

3 Lecture 3 Jan 11th

3.1 Sylow Theory (Continued)

Lemma 9 (Counting The Conjugates of a Sylow p-Subgroup)

Let G be a finite group, and p a prime such that $p \mid |G|$. Let

- *P be a Sylow p-subgroup;*
- *Q be a p-subgroup;*
- *$K = \left\{gPg^{-1} \mid g \in G\right\}$;*
- *Q act on K by conjugation; and*
- *$P = P_1, P_2, \ldots, P_r$ be the distinct orbit representatives from the action of Q on K.*

Then

$$|K| = \sum_{i=1}^{r} [Q : Q \cap P_i] .$$

Proof

From the definition of K, and the fact that Q acts on K, we have

$$\begin{aligned}
|K| &= \sum_{i=1}^{r} |\text{orb}(P_i)| \\
&= \sum_{i=1}^{r} |Q| \,/\, |\text{stab}(P_i)| \quad \text{orbit-stabilizer} \\
&= \sum_{i=1}^{r} |Q| \,/\, |N_G(P_i) \cap Q| \quad \text{by the action} \\
&= \sum_{i=1}^{r} [Q : N_G(P_i) \cap Q] \quad \text{by definition} \\
&= \sum_{i=1}^{r} [Q : Q \cap P_i] \quad \text{the last lemma.}
\end{aligned}$$

[1]

□

[1] Why can we use Lemma 8? Are the P_i's Sylow p-subgroups?

Theorem 10 (Second Sylow Theorem)

If P and Q are Sylow p-subgroups of G, then $\exists g \in G$ such that $P = gQg^{-1}$.

Proof

Let $K = \{qPq^{-1} \mid q \in G\}$. WTS $Q \in K$. We shall also note that $|P| = p^k$ for some $k \in \mathbb{N}$.

Let P act on K by conjugation. Let the orbit representatives be

$$P = P_1, P_2, \ldots, P_r.$$

By Lemma 9, we have

$$|K| = \sum_{i=1}^{r} [P : P \cap P_i] = [P : P] + \sum_{i=2}^{r} [P : P \cap P_i] = 1 + \sum_{i=2}^{r} [P : P \cap P_i].$$

Thus

$$|K| \equiv 1 \mod p.$$

Now let Q act on K by conjugation. Reordering if necessary, the

orbit representatives are

$$P = P_1, P_2, \dots, P_s,$$

where s is not necessarily r. From here, it suffices to show that $Q = P_i$ for some $i \in \{1, 2, \dots, s\}$. Suppose not. Then by Lemma 9,

$$|K| = \sum_{i=1}^{s} [Q : P_i \cap Q].$$

Note that it must be the case that $[Q : P_i \cap Q] > 1$, for some if not all i, for otherwise it would imply that $Q \cap P_i$ and that would be a contradiction. Then by Lagrange,

$$|K| \equiv 0 \mod p.$$

This contradicts the fact that $|K| \equiv 1 \mod p$.

This shows that $Q = P_i$ for some $i \in \{1, 2, \dots, s\}$, and so Q is a conjugate of P. □

Note 3.1.1 (Notation)

We shall denote n_p as the number of Sylow p-subgroups in G.

Theorem 11 (Third Sylow Theorem)

Let p be a prime, and that it divides $|G|$, where G is a group. Suppose $|G| = p^n m$, where $n, m \in \mathbb{N}$ and $p \nmid m$. Then

1. $n_p \equiv 1 \mod p$; *and*
2. $n_p \mid m$.

Proof

Let P be a Sylow p-subgroup of G, and let

$$K = \left\{ gPg^{-1} \;\middle|\; g \in G \right\}.$$

By Sylow's second theorem, $n_p = |K|$ as all the conjugates are exactly the Sylow p-subgroups. And by our last proof, we saw that $n_p \equiv 1 \mod p$.

Let G act on K by conjugation. Then by the Orbit-Stabilizer Theorem,

$$|G| = |\text{stab}(P)|\,|\text{orb}(P)|\,.$$

Thus

$$p^n m = |N_G(P)|\, n_p. \tag{3.1}$$

Thus $n_p \mid p^n m$. Since $n_p \equiv 1 \not\equiv 0 \mod p$, we must have $n_p \mid m$. □

Remark 3.1.1

1. *From Equation (3.1), we have that*

$$n_p = [G : N_G(P)].$$

2. ★ *Note that*

$$n_p = 1 \iff \forall g \in G\ gPg^{-1} = P \iff P \triangleleft G.$$

*However, note that P **may be trivial**! This means that if G is simple, it does not imply that $n_p = 1$.*

Definition 5 (Simple Group)

*A group is said to be **simple** if it has no non-trivial[2] normal subgroups.*

[2] By non-trivial, we mean that the normal subgroup is not the group with only the identity element.

Example 3.1.1

Prove that there is no simple group of order 56.

Proof

Let G be a group. Note that $56 = 2^3 \cdot 7$. Then $n_7 \equiv 1 \mod 7$ and

(No simple subgroup of order n)

The approach to showing that there are no simple groups of a certain order is as follows:

- *we make use of the fact that each group has a Sylow subgroup, and there are usually not many such subgroups;*
- *using each of the possiblities as cases, we find out if a group of the given order will have a normal subgroup.*

$n_7 \mid 8 = 2^3$. Thus

$$n_7 = 1 \text{ or } n_7 = 8.$$

$n_7 = 1$ By the remark above, G has a normal Sylow 7-subgroup. Thus G is not simple.

$n_7 = 8$ By Lagrange, since 7 is prime [3], the distinct Sylow 7-subgroups of G intersect trivially. Therefore, there are $8 \times 6 = 48$ elements of order 7 in G. But this implies that $56 - 48 = 8$ elements that are not of order 7. One of them is the identity, thus the remaining 7 elements must have order 2 [4]. This implies that

$$n_2 = 7 \equiv 1 \mod 2,$$

which by our remark means that G has a normal Sylow 2-subgroup. Thus G is not simple by both accounts. □

[3] This makes use of the fact that the Sylow 7-subgroup has a prime order, not just because 7 itself is prime. We say this here because if the order of the Sylow p-subgroup is prime, then by Lagrange, $|P \cap Q|$, where P and Q are distinct Sylow p-subgroups, is a subgroup of P (and Q), and must hence either be 1 or p. But this intersection cannot have order p, since P and Q are distinct. Thus $|P \cap Q| = 1$.

It is also important to note that this is only true if the order of the Sylow p-subgroups are prime, i.e. simply p itself. If their orders are p^n for some $n > 1$, this is not necessarily true.

[4] They cannot be of any other order as that would create a cyclic group that is not of order 2 or 7, which is impossible.

4 Lecture 4 Jan 14th

4.1 Sylow Theory (Continued 2)

Remark 4.1.1

1. *Let $p \neq q$ both be primes, and $p, q \mid |G|$. Let H_p and H_q be a Sylow p-subgroup and a Sylow q-subgroup of G, respectively. By Lagrange's Theorem, we must have that $H_p \cap H_q = \{e\}$. Then*

$$\left|H_p \cup H_q\right| = \left|H_p\right| + \left|H_q\right| - 1.$$

2. *Let $|G| = pm$ and $p \nmid m$, where p is prime. If H, K are Sylow p-subgroups of G with $H \neq K$, then $H \cap K = \{e\}$.*

Example 4.1.1

Let $G = D_6$. Notice that

$$H = \langle 1, s\rangle, \quad K = \langle 1, rs\rangle$$

are both Sylow 2-subgroups of D_6 and $H \neq K$, and their intersection is trivial.

Example 4.1.2

Let $|G| = pq$ where p, q are primes with $p < q$ and $p \nmid q - 1$. Then $|G|$ is cyclic.

Proof

By the Third Sylow Theorem, $n_p \equiv 1 \mod p$ and $n_p \mid q$. Notice that

$n_p = 1$, since if $n_p = q$, then $n_p \equiv 1 \mod p \implies p \mid q-1$, contradicting our assumption. By our remark last lecture, G has a normal Sylow p-subgroup, which we shall call H_p.

On the other hand, $n_q \equiv 1 \mod q$ and $n_q \mid p$. Since $p < q$, $q \nmid p-1$, and so the same argument as before holds. Hence $n_q = 1$, and so G has a normal Sylow q-subgroup.

Since $H_p \triangleleft G$, we know that $H_pH_q \leq G$, and we notice that

$$\left|H_pH_q\right| = \frac{\left|H_p\right|\left|H_q\right|}{\left|H_p \cap H_q\right|} = pq = |G|.$$

Thus $G = H_pH_q$. Let $a, b \in G$. If a, b is either both in H_p or both in H_q, then $ab = ba$ [1]. WMA $a \in H_p$ and $b \in H_q$. By our first remark today, note that $H_p \cap H_q = \{e\}$. Then, observe that

[1] Note: H_p and H_q are normal subgroups.

$$\underbrace{aba^{-1}}_{H_q} \underbrace{b^{-1}}_{H_q} \in H_q \qquad \underbrace{a}_{H_p} \underbrace{ba^{-1}b^{-1}}_{H_p} \in H_p$$

Thus $aba^{-1}b^{-1} = e \implies ab = ba$. So G is abelian. By the Fundamental Theorem of Finite Abelian Groups

$$G \simeq \mathbb{Z}_p \times \mathbb{Z}_q \simeq \mathbb{Z}_{pq},$$

which is cyclic. □

Example 4.1.3

By the Fundamental Theorem of Finite Abelian Groups

$$S_3 \simeq \mathbb{Z}_2 \times \mathbb{Z}_3,$$

and $|S_3| = 6 = 2 \cdot 3$, is not cyclic. Notice that S_3 does not fulfill the requirements for the last example since $2 \mid 3-1 = 2$.

Example 4.1.4

If $|G| = 30$, then G has a subgroup isomorphic to $\mathbb{Z}_{15}$. Note that $|G| = 2 \cdot 3 \cdot 5$. By the Third Sylow Theorem,

$$n_5 \equiv 1 \mod 5 \text{ and } n_5 \mid 6 \implies n_5 = 1 \text{ or } 6$$

and

$$n_3 \equiv 1 \mod 3 \text{ and } n_3 \mid 10 \implies n_3 = 1 \text{ or } 10.$$

Suppose $n_5 = 6$ and $n_3 = 10$. Since the Sylow 3-subgroups and Sylow 5-subgroups intersect trivially, this accounts for $(6 \times 4) + (10 \times 2) = 44$ elements but $|G| = 30 < 44$. Thus we must have $n_5 = 1$ or $n_3 = 1$. Thus G is not simple.

Let H_3 and H_5 be Sylow 3- and 5-subgroups, respectively. WLOG, suppose $H_3 \triangleleft G$. Then $H_3H_5 \leq G$, and notice that $|H_3H_5| = 15$. Since $15 = 3 \cdot 5$ and $3 \nmid 4 = 5 - 1$, we know that $H_3H_5 \simeq \mathbb{Z}_{15}$ by an earlier example.

Example 4.1.5

Let $|G| = 60$ with $n_5 > 1$. Then G is simple.

This is an important example for it is with this that we can prove the following:

Corollary 12 (A_5 is Simple)

A_5 is simple.

Proof

Note that $|A_5| = \frac{5!}{2} = 60$, and

$$\left\langle \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \end{pmatrix} \right\rangle \text{ and } \left\langle \begin{pmatrix} 1 & 3 & 2 & 4 & 5 \end{pmatrix} \right\rangle$$

are both Sylow 5-subgroups that are distinct (one has odd **parity** while the other has even). □

Proof (For Example 4.1.5)

Suppose $n_5 > 1$. Notice that $60 = 2^2 \cdot 3 \cdot 5$. By Theorem 11, $n_5 \equiv 1 \mod 5$ and $n_5 \mid 12$, and thus $n_5 = 6$. This accounts for $6 \times 4 + 1 = 25$ elements. Now suppose $H \triangleleft G$ is proper and non-trivial.

If $5 \mid |H|$, then H contains a Sylow 5-subgroup of G. Since $H \triangleleft G$, H contains all the conjugates of this Sylow 5-subgroup. Thus by our argument above, we have that $|H| \geq 25$ [2]. Also, $H \mid 60$. Thus it must be that $|H| = 30$. But then by the last example, $n_5 = 1$, a contradiction.

So $5 \nmid |H|$. By Lagrange, it remains that

$$|H| = 2,\ 3,\ 4,\ 6 \text{ or } 12.$$

Case A $|H| = 12 = 2^2 \cdot 3$.[3] So H contains a normal Sylow 2- or 3-subgroup that is normal in G. □

[2] These are the 25 elements that were found in the last paragraph.

[3]

Exercise 4.1.1
Prove that either $n_2 = 1$ or $n_3 = 1$.

The proof shall be continued next lecture.

Part II

Fields

5 Lecture 5 Jan 14th

5.1 Sylow Theory (Continued 3)

We shall continue with the last proof from where we left off.

Proof (Example 4.1.5 continued)

Case A $|H| = 12$. WLOG, let K be a normal Sylow 3-subgroup of H, which is also normal in G [1].

Case B $|H| = 6$. H would then have a normal Sylow 3-subgroup, which is normal in G. We shall also call this subgroup K.

By replacing H with K if necessary, wma $|H| \in \{2,3,4\}$. Consider $\overline{G} = G/H$. Then $|\overline{G}| \in \{15,20,30\}$. [2] In any case, $\overline{G}$ has a normal Sylow 5-subgroup. Call this normal subgroup $\overline{P}$. By correspondence, $\overline{P} = P/H$ where P is a normal subgroup of G [3]. Thus P is a proper non-trivial normal subgroup of G. Also,

$$|P| = |\overline{P}| \cdot |H| = 5 \cdot |H|.$$

Thus $5 \mid |P|$, putting us back to the case where $5 \mid |H|$. Thus G does not have a non-trivial normal subgroup, i.e. G is simple. □

[1] In Sylow Theory, normality is transitive:

Proof

If P is a normal Sylow p-subgroup of G, and Q is a normal subgroup of P, then $\forall q \in Q$, we have $q \in P$ and so $gqg^{-1} = q$ by normality of P. It follows that $gQg^{-1} = Q$ and so Q is also normal in G. □

[2]

Exercise 5.1.1
Prove that $\overline{G}$ has a normal Sylow 5-subgroup in all the three possible orders of $\overline{G}$.

[3] Note: correspondence works for the normal case as well.

5.2 Review of Ring Theory

Let F be a **field**, and I be an **ideal** of $F[x]$, its **polynomial ring**. Since $F[x]$ is a PID, we have $I = \langle p(x) \rangle$ for some $p(x) \in F[x]$.

Moreover, I is **maximal** iff $p(x)$ is **irreducible**.

Thus we observe that

$F[x]/I$ is a field iff $I = \langle p(x) \rangle$ is maximal iff $p(x) \in F[x]$ is irreducible.

Therefore, to talk about fields, we need to understand irreducibles.

5.3 Irreducibles

Definition 6 (Irreducible)

Let R be an integral domain (ID) [4]*. We say that $f(x) \in R[x]$ is **irreducible** (over R) if*

1. $f(x) \neq 0$;
2. $f(x) \notin R^\times$, *where $R^\times$ is the set of units of R;*
3. *whenever $f(x) = g(x)h(x)$, where $g(x), h(x) \in R[x]$, then either $g(x) \in R^\times$ or $h(x) \in R^\times$.*

*If $f(x) \neq 0$, $f(x) \notin R^\times$ and $f(x)$ is not irreducible, we say that $f(x)$ is **reducible** (over R).*

[4] **Integral domains** are commutative rings that has no zero divisors.

Example 5.3.1

$f(x) = x^2 - 2$ is irreducible over $\mathbb{Q}$ but reducible over $\mathbb{R}$ as

$$f(x) = \left(x - \sqrt{2}\right)\left(x + \sqrt{2}\right).$$

Let F be a field, $f(x) \in F[x]$ and $a \in F$. By the **Division Algorithm**, we can write

$$f(x) = (x - a)q(x) + r(x),$$

where $q(x), r(x) \in F[x]$. Note that we either have $r(x) = 0$ or $\deg r < \deg(x - a) = 1$. In the latter case, $r \in F$, and so

$$f(x) = (x - a)q(x) + r.$$

Then $f(a) = 0 + r = r$, and so $f(x) = (x - a)q(x) + f(a)$.

$$\therefore (x - a) \mid f(x) \iff f(a) = 0.$$

Proposition 13 (Polynomials with Roots are Reducible)

Let F be a field. If $f(x) \in F[x]$ with $\deg f > 1$, and f has a root in F, then f is reducible (over F).

Example 5.3.2

Let $f(x) = x^6 + x^3 + x^4 + x^3 + 3 \in \mathbb{Z}_7[x]$. Then $f(1) = 0$. Therefore

$$f(x) = (x-1)g(x) \text{ where } g(x) \in \mathbb{Z}_7[x].$$

Thus $f(x)$ is reducible over $\mathbb{Z}_7$.

Proposition 14 (Irreducible Rootless Polynomials)

Let F be a field[5]*. If $f(x) \in F[x]$ with $\deg f \in \{2,3\}$, then $f(x)$ is irreducible over F iff $f(x)$ has no roots in F.*

[5] Note that this does not work in an ID. For example, $2x^2 + 2$.

Warning

$(x^2+1)^2 \in \mathbb{R}[x]$ *is reducible but has no root in* $\mathbb{R}$. *Note that the degree of the polynomial is* 4.

Example 5.3.3

Let $f(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$. Note that $f(0) = 1$ and $f(1) = 3 \equiv 1 \mod 2$. Since $\deg f = 3$ and f has no roots in $\mathbb{Z}_2$, $f(x)$ is irreducible over $\mathbb{Z}_2$.

Theorem 15 (Gauss' Lemma)

Let R be a Unique Factorization Domain (UFD), with field of fractions F. Let $p(x) \in R[x]$. If

$$p(x) = A(x)B(x),$$

where $A(x), B(x)$ are non-constant in $F[x]$, then $\exists r, s \in F^\times$ non-zero such that

$$p(x) = a(x)b(x),$$

where $a(x) = rA(x)$ and $b(x) = sB(x)$.

Note 5.3.1

If $p(x) \in R[x]$ is reducible over F, then $p(x)$ is reducible over R.

Note 5.3.2

If $R = \mathbb{Z}$ and $F = \mathbb{Q}$, then $p(x)$ is irreducible over $\mathbb{Z}$, then $p(x)$ is irreducible over $\mathbb{Q}$.

---

6 Lecture 6 Jan 18th

6.1 Irreducibles (Continued)

Our goal in this section is to develop methods to test for the irreducibility of polynomials.

Warning

Note that $f(x) = 2x+4 = 2(x+2)$ *is reducible ovver* $\mathbb{Z}$ [1] *but irreducible over* $\mathbb{Q}$.

[1] This is interesting over $\mathbb{Z}$, since $2 \notin \mathbb{Z}^\times$.

Proposition 16 (Mod-p Irreducibility Test)

Let $f(x) \in \mathbb{Z}[x]$ *with* $\deg f \geq 1$. *Let* $p \in \mathbb{Z}$ *be prime. If* $\bar{f}(x)$ *is the corresponding polynomial in* $\mathbb{Z}_p[x]$ *such that*

- *the coefficients of* $\bar{f}(x)$ *are coefficients of* $f(x)$ *in mod* p,
- $\deg f = \deg \bar{f}$ [2], *and*
- $\bar{f}$ *is irreducible over* $\mathbb{Z}_p$,

then $f(x)$ *is irreducible over* $\mathbb{Q}$.

[2] This means that the leading coefficient of f is not killed off.

Proof

Suppose $\deg f = \deg \bar{f}$, and $\bar{f}(x) \in \mathbb{Z}_p$ is irreducible over $\mathbb{Z}_p$. Suppose to the contrary that $f(x)$ is reducible over $\mathbb{Q}$. Then for some

$g(x), h(x) \in \mathbb{Q}[x]$ with $\deg g, \deg h < \deg f$, we have

$$f(x) = g(x)h(x).$$

By Gauss' Lemma, wma $g(x), h(x) \in \mathbb{Z}[x]$. Then we have

$$\bar{f}(x) = \bar{g}(x)\bar{h}(x) \in \mathbb{Z}_p[x].$$

By assumption, $\bar{f}$ is irreducible over $\mathbb{Z}_p$, either

$$\deg \bar{g} = 0 \text{ or } \deg \bar{h} = 0.$$

Wlog, $\deg \bar{g} = 0$. Then

$$\deg h \leq \deg f = \deg \bar{f} = \deg \bar{h} \leq \deg h,$$

which implies that $\deg f = \deg h$ but $\deg h < \deg f$. Thus f is irreducible over $\mathbb{Q}$. □

Example 6.1.1

Consider the polynomial

$$f(x) = 3x^3 + 22x^2 + 17x + 471.$$

Then consider

$$\bar{f}(x) = x^3 + x + 1 \in \mathbb{Z}_2[x].$$

Since $\bar{f}(0) \neq 0$ and $\bar{f}(1) \neq 0$, and $\deg f = 3$, by Proposition 14, $\bar{f}(x)$ is irreducible over $\mathbb{Z}_2$. Since $\deg f = \deg \bar{f}$, f is irreducible over $\mathbb{Q}$ by the Mod-2 irreducible test.

Warning

*Consider $f(x) = 2x^2 + x \in \mathbb{Q}[x]$, which is reducible over $\mathbb{Q}$. However, $\bar{f}(x) = x \in \mathbb{Z}_2[x]$ is **reducible** over $\mathbb{Z}_2$. Notice here that $\deg \bar{f} \neq \deg f$.*

More generally so...

Proposition 17 (Polynomials that Cannot be Factored Over the Ideals is Irreducible)

Let I be a proper ideal of an ID R. Let $p(x) \in R[x]$ be monic and non-const. If $p(x)$ cannot be factored in $(R/I)[x]$ [3] into polynomials of lesser degree, then $p(x)$ is irreducible over R.

[3] Note that (R/I) may not be an ID even if R is one.

Proof

Sps to the contrary that $p(x)$ is reducible over R. Then

$$p(x) = f(x)g(x)$$

for some $f(x), g(x) \notin R^\times$. Since $p(x)$ is monic, and $\deg f, \deg g < \deg p$, wma $f(x)$ and $g(x)$ are also monic. Then

$$\bar{p}(x) = \bar{f}(x)\bar{g}(x) \in (R/I)[x].$$

Since $I \subsetneq R$, we have that $1 \notin I$, and so

$$\deg \bar{f}, \deg \bar{g} < \deg \bar{p}$$

but that implies that $p(x)$ can be factored in $(R/I)[x]$. □

Proposition 18 (Eisenstein's Criterion)

Let R be an ID. Let P be a prime ideal of R. Let

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in R[x]$$

with $n \geq 1$. Note that f is monic. Now if

$$a_{n-1}, a_{n-2}, \ldots, a_1, a_0 \in P \text{ and } a_0 \notin P^2,$$

then f is irreducible over R.

Proof

Sps to the contrary that f is reducible over R. Since $f(x)$ is monic,

$$f(x) = g(x)h(x)$$

where $g(x), h(x) \in R[x]$ and $\deg g, \deg h < \deg f$. Then

$$\bar{f}(x) = \bar{g}(x)\bar{h}(x) = x^n \in (R/P)[x]$$

since $a_{n-1}, a_{n-2}, \ldots, a_1, a_0 \in P$. Since P is prime, R/P is an ID, we have that either $\bar{g}(0) = 0$ or $\bar{h}(0) = 0$. Wlog, $\bar{g}(0) = 0 \in P$. But that implies that $a_0 = \bar{g}(0)\bar{h}(0) = 0 \in P^2$, a contradiction. □

7 Lecture 7 Jan 21st

7.1 Irreducibles (Continued 2)

Example 7.1.1

Prove that $f(x,y) = x^2 + y^2 - 1$ is irreducible in $\mathbb{Q}[x,y] = (\mathbb{Q}[x])[y]$.

Proof

Let $g(y) = y^2 + (x^2+1)$. Since $x+1$ is irreducible, let $P = \langle x+1 \rangle$, which is therefore a prime ideal of $\mathbb{Q}[x]$. Moreover, notice that

$$x^2 - 1 = (x+1)(x-1) \in P.$$

Since $(x+1)^2 \nmid (x^2-1)$, we have that $x^2 - 1 \notin P^2$. Then by Eisenstein, we have that $f(x,y)$ is irreducible. □

Corollary 19 (Eisenstein + Gauss)

Let $p \in \mathbb{Z}$ be a prime, and let

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

be non-const in $\mathbb{Z}[x]$. If $p \mid a_i$ for all $i \in \{0, \ldots, n-1\}$, and $p^2 \nmid a_0$, then f is irreducible over $\mathbb{Q}$.

Recall that the prime ideals of $\mathbb{Z}$ are $\mathbb{Z}_p$ where p is prime.

Proof

Let $P = \langle p \rangle$. It follows from Eisenstein that f is irreducible over $\mathbb{Z}$, and then from Gauss that f is irreducible over $\mathbb{Q}$. □

Example 7.1.2

Let $f(x) = x^n - d \in \mathbb{Z}[x]$ where $\exists p \in \mathbb{Z}$ prime such that $p^2 \nmid d$ and $p \mid d$. Let $P = \langle p \rangle$ and so by Corollary 19, f is irreducible over $\mathbb{Q}$.

Note 7.1.1

The above example is noteworthy since it will appear rather often throughout this course. Notice that if we have polynomials of the above form, then we immediately have that the polynomial is irreducible.

Example 7.1.3

Are the following irreducible over $\mathbb{Q}$?

1. $f(x) = x^7 + 21x^5 + 15x^2 + 9x + 6$

   Yes. Notice that all the non-leading coefficients have a factor of 3, and so if we let $p = 3$, since $3^2 = 9 \nmid 6$, it follows from Eisenstein that f is irreducible over $\mathbb{Q}$.

2. $f(x) = x^3 + 2x + 16$

   Eisenstein can't help us here since $\gcd(2, 16) = 2$ and $2^2 = 4 \mid 16$. Consider $\bar{f}(x) = x^3 + 2x + 1 \in \mathbb{Z}_3[x]$. Notice that $\bar{f}(0) = 1 = \bar{f}(2)$ and $\bar{f}(1) = 4$. Since $\deg \bar{f} = 3$, it follows from Proposition 14 that $\bar{f}$ is irreducible over $\mathbb{Z}_3$. Since $\deg f = \deg \bar{f}$, it follows from the Mod-3 irreducible test that f is irreducible over $\mathbb{Q}$.

3. $f(x) = x^4 + 5x^3 + 6x^2 - 1$

   Again, Eisenstein can't help us here, since $5 \perp 6 \perp 1$ [1]. Consider

   $$\bar{f}(x) = x^4 + x^3 + 1 \in \mathbb{Z}_2[x].$$

   We know that $\bar{f}(0) = 1 = \bar{f}(1)$, and so $\bar{f}$ has no roots in $\mathbb{Z}_2$. [2]

[1] $\perp$ is a common notation for coprimeness.

[2] Note that we cannot use Proposition 14 here as $\deg \bar{f} = 4 > 3$.

Consider the quadratics[3] of $\mathbb{Z}_2[x]$: we have

$$x^2, \quad x^2+x, \quad x^2+1, \quad x^2+x+1,$$

all, but the last, of which are reducible. However, notice that

$$\left(x^2+x+1\right)^2 = x^4+x^2+1 \neq \bar{f}(x)$$

(by the Freshman's Dream). Thus $\bar{f}$ is irreducible in $\mathbb{Z}_2$. Since $\deg f = \deg \bar{f}$, by Mod-2 irreducible test.

[3] **Why did we only check for the quadratics and not others?** We did so as we have already checked for the linear factors by checking for roots, which also checks for the cubic factors, since if we can factor out a linear factor, we are left with a cubic factor. Ruling out linear factors in turn rules out cubic factors.

4. ★ Let p be a prime, and let

$$f(x) = x^{p-1}+x^{p-2}+\ldots+x^2+x+1.$$

Note that $f(x)(x-1) = x^p-1$, and so $f(x) = \frac{x^p-1}{x-1}$. Furthermore, notice that

$$\begin{aligned} f(x+1) &= \frac{(x+1)^p-1}{x} = \sum_{k=0}^{p}\binom{p}{k}x^{p-k}-\frac{1}{x} \\ &= x^{p-1}+\binom{p}{p-1}x^{p-2}+\ldots+\binom{p}{2}x+\binom{p}{1}. \end{aligned}$$

By setting $P = \langle p\rangle$, we have that $f(x+1)$ is irreducible by Eisenstein. It follows from A3Q2 that $f(x)$ is also irreducible. ∎

7.1.1 *Summary for Proving Irreducibility*

(Summary for Proving Irreducibility) *This subsection is dedicated to summarize the ways that are available to us to finding out if a given polynomial is reducible or irreducible. This includes common heuristics and/or techniques.*

Showing reducibility Let $f(x) \in F[x]$. $f(x)$ is reducible if

- $f(x)$ **has a root** α **in** $F[x]$, because that means $x-\alpha \in F[x]$, and thus $x-\alpha \mid f(x)$.
- $f(x) = g(x)h(x)$ for some non-constant $g(x), h(x) \in F[x]$, which is just by definition.

Showing irreducibility Let $f(x) \in F[x]$. Note that it is possible to mix and match these tools to achieve our goal. Our trusty tools include:

- **Eisenstein**: find a prime or irreducible polynomial (prime ideals) such that
  - **each of the coefficients, except for the leading coefficient, is divisible**

by the prime (or irreducible), and

- **the square of the last coefficient is not divisible by the prime (or irreducible)**.

- If $\deg f \in \{2,3\}$, then by Proposition 14, we simply need to check that the polynomial does not have roots. This sounds crazy in an infinite field, but we can combine this with...

- **Mod-p irreducibility**: find the equivalent $\tilde{f}(x) \in \mathbb{Z}_p[x]$: that is, let $\tilde{f}(x) \in \mathbb{Z}_p[x]$ be such that we replace each of the coefficients of f are replaced with their counterparts in $\mathbb{Z}_p$. Then use the other methods here to check for irreducibility.

Some somewhat helpful heuristics that can reduce our work and/or make a problem much easier include:

- If our polynomial is of the form

$$f(x) = x^{2n} + a_{2n-2}x^{2n-2} + \ldots + a_2x^2 + a_0,$$

then we can let $y = x^2$ and consider the polynomial

$$g(y) = y^n + a_{2n-2}y^{n-1} + \ldots + a_2y + a_0.$$

Note that if $g(y)$ is reducible, then so is $f(x)$. Conversely, if we want $f(x)$ to be irreducible, it had better be the case that $g(y)$ is irreducible.

7.2 *Field Extensions*

Let K be a field. Recall that a non-empty subset $F \subseteq K$ is called a **subfield** of K if F is a field under the same operations.

Example 7.2.1

$\mathbb{Q}(\sqrt{2}) := \left\{a + b\sqrt{2} \;\middle|\; a,b \in \mathbb{Q}\right\}$ is a subfield of $\mathbb{C}$. We call this field $\mathbb{Q}$ '**adjoin**' $\sqrt{2}$.

Note 7.2.1

We did not actually show that $\mathbb{Q}(\sqrt{2})$ is indeed a field but note the follow-

ing: let $a+b\sqrt{2} \neq 0 \in \mathbb{Q}(\sqrt{2})$. Then

$$\frac{1}{a+b\sqrt{2}} \cdot \frac{(a-b\sqrt{2})}{(a-b\sqrt{2})} = \frac{a-b\sqrt{2}}{a^2-2b^2} \in \mathbb{Q}(\sqrt{2}),$$

and note that

$$a^2-2b^2 \neq 0 \iff \frac{a}{b} = \sqrt{2},$$

which does not happen in $\mathbb{Q}$ itself.

Definition 7 (Field Extension)

*Let F be a field. A **field extension** (or an **extension**) of F is a field K which contains an **isomorphic** copy of F as a subfield. We denote this notion of K/F.*

Example 7.2.2

- We have that $\mathbb{C}/\mathbb{R}$ and $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$.
- For a prime p, if

$$\mathbb{Z}_p(x) = \left\{ \frac{f(x)}{g(x)} \;\middle|\; f(x), g(x) \in \mathbb{Z}_p[x], g \neq 0 \right\},$$

  then $\mathbb{Z}_p(x)/\mathbb{Z}_p$.
- Let F be a field, and $f(x) \in F[x]$ be irreducible. Then let $K = F[x]/\langle f(x)\rangle$. Then K/F.
- Note that $\mathbb{Q}$ is not an extension of $\mathbb{Z}_p$ for any prime p.

Note 7.2.2

Note that in the last example, K is not a 'direct' extension of F, but it contains an isomorphic copy of F. This allows us to have more flexibility in what we can do.

Warning

If given $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$, then $\mathbb{Q}$ is not an extension of $\mathbb{Z}_p$ since the two use different operations.

8 Lecture 8 Jan 23rd

8.1 Field Extensions (Continued)

Example 8.1.1

Let F be a field.

- If the characteristic $ch(F) = p > 0$ is a prime, then

$$F \supset \{0, 1, 2, \dots, p-1\} \simeq \mathbb{Z}_p.$$

  Thus $F/\mathbb{Z}_p$.

- If $\mathrm{ch}(F) = 0$, then $F/\mathbb{Q}$.

In either of these cases, we call $\mathbb{Z}_p$ and/or $\mathbb{Q}$ the **prime subfield** of F.

Definition 8 (Generated Field Extension)

Let K/F, and $\alpha_1, \dots, \alpha_n \in K$. The field extension of F generated by $\{a_i\}_{i=1}^n$ is

$$F(\alpha_1, \dots, \alpha_n) := \left\{ \frac{f(\alpha_1, \dots, \alpha_n)}{g(\alpha_1, \dots, \alpha_n)} \;\middle|\; f, g \in F[x_1, \dots, x_n], g \neq 0 \right\},$$

of which we call as F adjoin $\alpha_1, \dots, \alpha_n$.

Note 8.1.1

We have that $F(\alpha_1, \dots, \alpha_n)/F$, and in turn $K/F(\alpha_1, \dots, \alpha_n)$.

Remark 8.1.1 (Minimality)

Let K/F, and $\alpha_1, \dots, \alpha_n \in K$. If we have E/F such that K/E and $\alpha_i \in E$ for all i, then

$$F(\alpha_1, \dots, \alpha_n) \subseteq E,$$

i.e. $F(\alpha_1, \dots, \alpha_n)$ is the smallest extension of F that contains the α_i's.

Example 8.1.2 (A classical example of field extensions)

Show that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

Proof

Since $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$, by closure, we have that $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$, and so $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

For the other direction, we have that $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Then in particular $\frac{1}{\sqrt{2}+\sqrt{3}} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Notice that

$$\frac{1}{\sqrt{2}+\sqrt{3}} \cdot \frac{\sqrt{2}-\sqrt{3}}{\sqrt{2}-\sqrt{3}} = \sqrt{3} - \sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3}).$$

So $2\sqrt{3}, 2\sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$ [1], and in turn $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Then by minimality, $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3})$. □

[1] $2\sqrt{2}$ follows from a similar argument by using $1 = \frac{\sqrt{3}-\sqrt{2}}{\sqrt{3}-\sqrt{2}}$.

Remark 8.1.2

Notice that $F(\alpha, \beta) = [F(\alpha)](\beta)$.

We have that $F(\alpha) \subseteq F(\alpha, \beta), \beta \in F(\alpha, \beta)$, which implies that $F(\alpha)(\beta) \subseteq F(\alpha, \beta)$ by minimality.

Also, since $F \subseteq F(\alpha, \beta)$, and $\alpha, \beta \in F(\alpha, \beta)$, we have, by minimality (again), that $F(\alpha, \beta) \subseteq F(\alpha)(\beta)$.

Proposition 20 (Span of the Extension)

Let K/F and $\alpha \in K$. If α is a root of some non-zero $f(x) \in F[x]$ irreducible over F, then $F(\alpha) \simeq F[x]/\langle f(x) \rangle$. Moreover, if $\deg f = n$,

then

$$F(\alpha) = \operatorname{span}_F\{1, \alpha, \ldots, \alpha^{n-1}\}.$$

Proof

Sps $\alpha \in K$ is a root of an irreducible $f(x) \in F[x]$ over F. Let $\deg f = n \in \mathbb{N}$. Define $\varphi : F[x] \to F(\alpha)$ by $\varphi(g(x)) = g(\alpha)$. Note that this is a ring homomorphism. Let

$$I = \{g(x) \in F[x] \mid g(\alpha) = 0\} = \ker \varphi,$$

which is an ideal. Since $F[x]$ is a PID [2], $\exists g(x) \in F[x]$ such that $I = \langle g(x) \rangle$. Since α is a root of $f(x)$, $f(x) \in I$, and so $f(x) = g(x)h(x)$ for some $h(x) \in F[x]$. Since $I \neq F[x]$ and f is irreducible, $h(x) \in F^\times$. Thus $\langle g(x) \rangle = \langle g(x) \rangle$. Then by the **First Isomorphism Theorem**,

$$F[x]/\langle f(x) \rangle \simeq \varphi(F[x]).$$

By construction, $\varphi(F[x]) \subseteq F(\alpha)$. Since $\varphi(F[x])$ is a field (by isomorphism) which contains $\alpha = \varphi(x)$ and F, and so by minimality $F(\alpha) \subseteq \varphi(F[x])$. Therefore

$$F[x]/\langle f(x) \rangle \simeq F(\alpha),$$

as required.

Through the isomorphism, for any $h(x) \in F[x]$, we have

$$h(x) + \langle f(x) \rangle \mapsto h(\alpha).$$

So

$$F[x]/\langle f(x) \rangle = \left\{ c_{n-1}x^{n-1} + \ldots + c_1 x + c_0 + \langle f(x) \rangle \;\middle|\; c_i \in F \right\}$$

and thus

$$\begin{aligned} F(\alpha) &= \left\{ c_{n-1}\alpha^{n-1} + \ldots + c_1\alpha + c_0 + \;\middle|\; c_i \in F \right\} \\ &= \operatorname{span}_F \left\{ 1, \alpha, \ldots, \alpha^{n-1} \right\}, \end{aligned}$$

as claimed. □

[2] See PMATH347.

9 Lecture 9 Jan 25th

9.1 Field Extensions (Continued 2)

Let K/F, and $0 \neq g(x) \in F[x]$, and $\alpha \in K$ such that $g(\alpha) = 0$. Since $F[x]$ is an ID, $g(x)$ must have an irreducible factor $f(x) \in F[x]$ such that $f(\alpha) = 0$. By the proof of Proposition 20,

$$\langle f(x) \rangle = \ker \varphi = I = \{h(x) \in F[x] \mid h(\alpha) = 0\}.$$

In particular,

- If $h(x) \in F[x]$ such that $h(\alpha) = 0$, then $h(x) \in \langle f(x) \rangle$. In particular, $f(x) \mid h(x)$.
- $\langle f(x) \rangle$ contains a unique, monic, irreducible polynomial: for any $g(x) \in \langle f(x) \rangle$ that is irreducible, we know that $g(x) = uf(x)$, where $0 \neq u \in F^\times$, and so we can just divide the polynomial g by u to make it monic.

Definition 9 (Minimal Polynomial)

*Let K/F, and $\alpha \in K$ be a root of a non-zero polynomial in $F[x]$. Then there exists a unique irreducible monic polynomial $f(x) \in F[x]$ such that $f(\alpha) = 0$. We call this $f(x)$ the **minimal polynomial** for α over F. If $\deg f = n$, we call n the **degree** of α over F, denoted $\deg_F(\alpha)$.*

Note 9.1.1

For an $\alpha \in K$, its minimal polynomial is unique, but a minimal polynomial

need not have only one root.

Proposition 21 (Span of an Extension if Linearly Independent)

Let K/F, and $\alpha \in K$ with minimal polynomial $f(x) \in F[x]$, with $\deg_F(\alpha) = n$. Then the span $F(\alpha) = \operatorname{span}_F\{1, \alpha, \dots, \alpha^{n-1}\}$ is linearly independent over F.

Proof

Sps to the contrary that

$$c_{n-1}\alpha^{n-1} + c_{n-2}\alpha^{n-2} + \dots + c_1\alpha + c_0 = 0,\ c_i \in F,$$

has a non-trivial solution, i.e. not all c_i's are 0 (i.e. we assume that the α's are linearly dependent). Consider

$$g(x) = c_{n-1}x^{n-1} + \dots + c_1 x + c_0,$$

and so $g \neq 0$. However, $g(\alpha) = 0$, so $g(x) \in \langle f(x) \rangle$, i.e. $f(x) \mid g(x)$. However, that contradicts the fact that $\deg f = n > n-1 \geq \deg g$. □

Example 9.1.1

Consider K/F, and $\alpha \in K$. Then

$$\deg_F(\alpha) = 1 \iff \text{min. polym } f(x) = x - \alpha \in F[x] \iff \alpha \in F.$$

Example 9.1.2

Consider $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. Let $\alpha = \sqrt{2}$. Note that $f(\alpha) = 0$ for $f(x) = x^2 - 2$, which is irreducible by Eisenstein by $P = \langle 2 \rangle$. Thus $\deg_F(\alpha) = 2$, and so

$$\mathbb{Q}(\sqrt{2}) = \operatorname{span}_{\mathbb{Q}}\{1, \alpha\} = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

Example 9.1.3

Let $\alpha = \sqrt{1+\sqrt{3}}$. Notice that $\alpha^2 = 1+\sqrt{3}$, and so $(\alpha^2-1)^2 = 3$. Thus

$$\alpha^4 - 2\alpha^2 + 1 - 3 = 0.$$

Let $f(x) = x^4 - 2x^2 - x \in \mathbb{Q}[x]$. Note that f is monic and $f(\alpha) = 0$. By Eisenstein, f is irreducible if we pick $P = \langle 2 \rangle$. Thus f is a minimal polynomial for α. We have that

$$\deg_{\mathbb{Q}}(\alpha) = \deg f = 4.$$

Example 9.1.4

Let $f(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$. Let α be a root of $f(x)$ in some extension of $\mathbb{Z}_2$. Compute the size of $\mathbb{Z}_2(\alpha)$.

Solution

We showed in one of our previous examples that such an f is irreducible in $\mathbb{Z}_2$. Thus $\deg_{\mathbb{Z}_2}(\alpha) = 3$. Then

$$\mathbb{Z}_2(\alpha) = \operatorname{span}_{\mathbb{Z}_2}\{1, \alpha, \alpha^2\},$$

where $\{1, \alpha, \alpha^2\}$ is linearly independent over $\mathbb{Z}_2$. Thus

$$|\mathbb{Z}_2(\alpha)| = 2 \times 2 \times 2 = 8.$$

Note 9.1.2

Notice that there is no guarantee that such a root exists, but it does, which is a theorem that we shall prove later. (See Theorem 28)

Corollary 22 (Isomorphism between Extensions)

Let K/F and $\alpha, \beta \in K$ have the same minimal polynomial $f(x) \in F[x]$. Then $F(\alpha) \simeq F(\beta)$.

Proof

From Proposition 20, we have that

$$F(\alpha) \simeq F[x]/\langle f(x)\rangle \simeq F(\beta).$$

□

10 Lecture 10 Jan 28th

10.1 Field Extensions (Continued 3)

How can we work with field extensions algebraically?

10.1.1 Linear Algebra on Field Extensions

We can look at K/F as K being an F-vector space.

Definition 10 (Finite Extension)

*We say K/F is a **finite extension** if K is a finite dimensional F-vector space. We call the dimension, $\dim_F K$, the **degree** of K/F, and denote this dimension as*

$$[K : F].$$

Example 10.1.1

We have $[\mathbb{C} : \mathbb{R}] = |\{1, i\}| = 2$.

Example 10.1.2

$[\mathbb{R} : \mathbb{Q}] = \infty$.

Example 10.1.3

Let K/F and $\alpha \in K$ with the minimal polynomial $f(x) \in F[x]$. Then $[F(\alpha) : F] = \left|\{1, \alpha, \ldots, \alpha^{n-1}\}\right| = n$, where $n = \deg f = \deg_F(\alpha)$.[1]

[1] This is why we call the dimension of K/F as a degree.

Definition 11 (Tower of Fields)

We say $F_1/F_2/F_3/\ldots/F_n$ is a tower of fields if each F_i/F_{i+1} is a field extension.

Theorem 23 (Tower Theorem)

If K/E and E/F are finite extensions, then

$$[K:F] = [K:E][E:F].$$

Proof

Let $\mathcal{B}_v = \{v_1, \ldots, v_n\}$ be a basis for K/E and $\mathcal{B}_w = \{w_1, \ldots, w_m\}$ be a basis for E/F.

Claim The set $\{v_i w_j :: 1 \leq i \leq n, 1 \leq j \leq m\}$ is a basis for K/F.

Linear Independence Assume

$$\sum_{i,j} c_{i,j} w_j v_i = 0. \tag{10.1}$$

Notice that we may write Equation (10.1) as

$$\sum_i \left(\sum_j c_{i,j} w_j \right) v_i = 0.$$

Since $\mathcal{B}_v$ is a basis of K/E, for each i, we have

$$\sum_j c_{i,j} w_j = 0.$$

Since $\mathcal{B}_w$ is a basis for E/F, for each j, we have

$$c_{i,j} = 0.$$

It follows that the $w_j v_i$'s are linearly independent of each other.

Span Let $u \in K$. Then

$$u = \sum_{i=1}^{n} c_i v_i,$$

where $c_i \in E$ is given by

$$c_i = \sum_{j=1}^{m} d_{i,j} w_j.$$

Then

$$u = \sum_{i,j} d_{i,j} w_j v_i.$$

Thus $\{v_i, w_j\}$ is a basis for K/F. □

Example 10.1.4

Compute $[\mathbb{Q}(\sqrt[3]{5}, i) : \mathbb{Q}]$.

Solution

By the Tower Theorem, we have that

$$[\mathbb{Q}(\sqrt[3]{5}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{5})(i) : \mathbb{Q}(\sqrt[3]{5})] \cdot [\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}].$$

Notice that

$$[\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}] = \deg(x^3 - 5) = 3.$$

For $[\mathbb{Q}(\sqrt[3]{5})(i) : \mathbb{Q}(\sqrt[3]{5})]$, let $p(x)$ be the minimal polynomial for i over $\mathbb{Q}(\sqrt[3]{5})$. Since $i^2 + 1 = 0$, we know that i is a root of $x^2 + 1 = 0$. Then in particular, we must have $p(x) \mid x^2 + 1$. So $\deg p \in \{1, 2\}$.

Now since $\mathbb{Q}(\sqrt[3]{5}) \subseteq \mathbb{R}$ and $i \notin \mathbb{Q}(\sqrt[3]{5})$, we observe that $\deg p \neq 1$. Thus $\deg p = 2$. It follows that

$$[\mathbb{Q}(\sqrt[3]{5})(i) : \mathbb{Q}(\sqrt[3]{5})] = 2.$$

Therefore

$$[\mathbb{Q}(\sqrt[3]{5}, i) : \mathbb{Q}] = 2 \cdot 3 = 6.$$

10.1.2 *Polynomials on Field Extensions*

Definition 12 (Algebraic and Transcendental)

*Let K/F. We say that $\alpha \in K$ is **algebraic** over F if $\exists 0 \neq f(x) \in F[x]$ such that $f(\alpha) = 0$. Otherwise, we say that α is **transcendental** over F; that is, there is no non-zero polynomial over F such that α is a root.*

We say that K/F is algebraic if every $\alpha \in K$ is ***algebraic*** *over F. Otherwise, we say that K/F is* ***transcendental****.*

Example 10.1.5

π is transcendental over $\mathbb{Q}$ [2]. However, π is algebraic over $\mathbb{R}$ (note that $x - \pi \in \mathbb{R}[x]$.).

[2] The proof of this statement is beyond our power at this point.

Example 10.1.6

As a direct consequence of the above example, we have that $\mathbb{R}/\mathbb{Q}$ is transcendental.

Example 10.1.7

As we have seen numerous times, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is algebraic.

Remark 10.1.1

If $\alpha \in K$ is algebraic over F, then α has a minimal polynomial in $F[x]$.

Theorem 24 (Finite Extensions are Algebraic)

If K/F is finite, then K/F is algebraic.

Proof

Suppose $[K : F] = n < \infty$. Let $\alpha \in K$. Consider

$$\alpha, \alpha^2, \ldots, \alpha^n, \alpha^{n+1}.$$

The idea is to make use of the fact that the extension will at least have the algebraic number as a span up to some degree n, and instead of working with the spanning set, we work with one α away. There will be two cases, each of which can be dealt with at relative ease.

Case 1 Suppose $\alpha^i = \alpha^j$ for some $i \neq j \in \{1, \ldots, n+1\}$. Then α is certainly a root of $f(x) = x^i - x^j$.

Case 2 Suppose $\alpha^i \neq \alpha^j$ for all $i \neq j$. Then we must have that

$$\alpha, \alpha^2, \ldots, \alpha^n, \alpha^{n+1}$$

is linearly dependent over F. Thus we may have

$$c_1\alpha + c_2\alpha^2 + \ldots + c_{n+1}\alpha^{n+1} = 0$$

where not all c_i's are 0. Then α is a root of

$$f(x) = c_{n+1}x^{n+1} \ldots + c_1 x,$$

which is a non-zero polynomial.

In either case, we observe that α is algebraic over F. Therefore K/F is algebraic. □

11 Lecture 11 Jan 30th

11.1 Field Extensions (Continued 4)

11.1.1 Polynomials on Field Extensions (Continued)

Note 11.1.1

Recall that given K/F,

- *Finite (defn):* $\dim_F K = [K : F] < \infty$
- *Algebraic (defn) :* $\forall \alpha \in K, \exists 0 \neq f \in F[x]$, *such that* $f(\alpha) = 0$
- *Finite* $\implies$ *Algebraic*

Definition 13 (Finitely Generated Extension)

We say K is a ***finitely generated extension*** *of F if $\exists \alpha_1, \alpha_2, \ldots, \alpha_n \in K$ such that $K = F(\alpha_1, \ldots, a_n)$.*

Proposition 25 (Finitely Generated Algebraic Extensions are Finite)

If K is a finitely generated algebraic extension of F, then K/F is finite.[1]

[1] This proposition is actually an **iff** statemnt in disguise.

Proof

Sps K/F is algebraic, where $K = F(\alpha_1, \ldots, \alpha_n)$. We shall proceed by

performing induction on n. If $n = 1$, then $[F(\alpha_1) : F] = \deg_F(\alpha_1) < \infty$.

Now suppose that the result holds for n. Consider

$$K = F(\alpha_1, \ldots, \alpha_n, \alpha_{n+1}).$$

Then by the Tower Theorem,

$$\begin{aligned}&[F(\alpha_1, \ldots, \alpha_n, \alpha_{n+1}) : F] \\ &= [F(\alpha_1, \ldots, \alpha_n)(\alpha_{n+1}) : F(\alpha_1, \ldots, \alpha_n)] \cdot [F(\alpha_1, \ldots, \alpha_n) : F].\end{aligned}$$

It follows from the base case and the induction hypothesis that

$$[F(\alpha_1, \ldots, \alpha_{n+1}) : F]$$

is finite. □

Note 11.1.2

Finite extensions are, therefore, finitely generated.

Example 11.1.1

The field $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{4}, \ldots)$ is an algebraic extension of $\mathbb{Q}$ but it is not a finite extension.

Proposition 26 (Greater Algebraic Extensions)

If K/E and E/F are algebraic extensions, then K/F is an algebraic extension.

Proof

Let $\alpha \in K$. Since K/E is algebraic, α has a minimal polynomial in $E[x]$, say it is

$$p(x) = x^n + c_{n-1}x^{n-1} + \ldots + c_1 x + c_0.$$

Then α is algebraic over $F(c_{n-1},\dots,c_1,c_0)$. By the Tower Theorem,

$$[F(c_{n-1},\dots,c_1,c_0,\alpha) : F(c_{n-1},\dots,c_0)] < \infty,$$

and so $F(c_{n-1},\dots,c_1,c_0,\alpha) \subseteq E$.

Now $F(c_{n-1},\dots,c_0)/F$ is algebraic and finitely generated. So it follows from the Tower Theorem that

$$[F(c_{n-1},\dots,c_0,\alpha) : F] < \infty.$$

Thus α is algebraic over F and so K/F is algebraic. □

Proposition 27 (Algebraic Numbers Form a Subfield)

Let K/F. The set of elements of K algebraic over F form a subfield of K.

Proof (Sketch proof)

Let $L = \{\alpha \in K : \alpha \text{ is alg. over } F\}$. Let $\alpha, \beta \in L$ and $\beta \neq 0$. Then

$$\alpha, \beta, \alpha+\beta, \alpha\beta, \beta^{-1} \in F(\alpha,\beta).$$

Then $[F(\alpha,\beta) : F] < \infty$ implies that L is finitely generated, which is thus algebraic, and is hence a subfield of K. □

11.2 Splitting Fields

From various examples in the past, we notice that many of the roots that we have come across live in $\mathbb{C}$. We shall see why later on, but we can ask ourselves if we can generalize this notion and make use of properties from this notion.

Definition 14 (Splits)

Let $f(x) \in F[x]$ be non-constant. We say $f(x)$ splits in an extension K/F

if there exists $\exists u \in F$, *and* $\exists \alpha_1, \ldots, \alpha_n \in K$ *such that*

$$f(x) = u(x - \alpha_1) \ldots (x - \alpha_n).$$

Example 11.2.1

Every non-constant polynomial in $\mathbb{R}[x]$ splits in $\mathbb{C}$.

Theorem 28 (Kronecker's Theorem)

Let $f(x) \in F[x]$ *be non-constant. There exists an extension* K/F *such that* $f(x)$ *has a root in* K.

Proof

Let $f(x) \in F[x]$ be non-constant. Then let $p(x) \in F[x]$ be an irreducible factor of $f(x)$. Then consider $K = F[t]/ < p(t) >$. which we know is a field. Then

$$\bar{t} = t + p(t) \in K$$

is a root of $p(x)$, which means that $\bar{t}$ is also a root for $f(x)$. □

Theorem 29 (Repeated Kronecker's Theorem)

Let $f(x) \in F[x]$ *be non-constant. Then there exists an extension* K/F *such that* $f(x)$ *splits over* K.

Proof

By the Fundamental Theorem of Algebra, if we suppose that $\deg f = n < \infty$, then f has n roots. Consequently, we need only to apply Theorem 28 for at most n-many times to get to an extension where $f(x)$ splits. □

---

12 Lecture 12 Feb 01st

12.1 Splitting Fields (Continued)

Definition 15 (Splitting Field)

*Let $f(x) \in F[x]$ be non-constant. A **minimal extension** K of F with the property that $f(x)$ splits over K is called a **splitting field** for $f(x)$ over F.*

The following result is a direct consequence of Theorem 29.

Proposition 30 (A Splitting Field is Generated)

Let $f(x) \in F[x]$ be non-constant, and let K/F be such that $f(x)$ splits over K. Suppose

$$f(x) = u(x - \alpha_1) \dots (x - \alpha_n),$$

where $u \in F$ and $\alpha_1, \dots, \alpha_n \in K$. Then a splitting field for $f(x)$ over F is $F(\alpha_1, \dots, \alpha_n)$.

Example 12.1.1

Find a splitting field for

$$f(x) = x^4 + x^2 - 6$$

over $\mathbb{Q}$.

Solution

Notice that

$$f(x) = (x^2+3)(x^2-2) = (x+\sqrt{3}i)(x-\sqrt{3}i)(x-\sqrt{2})(x+\sqrt{2})$$

in $\mathbb{C}[x]$. Then a splitting field of $f(x)$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{2}, \sqrt{3}i)$.

Now what if we had two differing extensions at which $f(x)$ splits, say K and E, and K and E are not the same field extension? In particular, K and E would contain some subfield, say $F(\alpha_1, \ldots, \alpha_n)$ and $F(\beta_1, \ldots, \beta_n)$ respectively, which may not be the same spliting field. How are these splitting fields related?

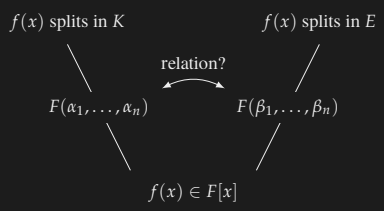

Figure 12.1: Differing Splitting Fields

Lemma 31 (Isomorphic Fields have Isomorphic Polynomial Rings)

Let F ad F' be fields. If $\varphi : F \to F'$ is an isomorphism, there exists a map $\tilde{\varphi} : F[x] \to F'[x]$ that is also an isomorphism.

Proof

The map $\tilde{\varphi} : F[x] \to F'[x]$ given by

$$\tilde{\varphi}(\alpha_n x^n + \ldots + \alpha_1 x + \alpha_0) = \tilde{\alpha}_n x^n \ldots + \tilde{\alpha}_1 x + \tilde{\alpha}_0$$

is clearly an isomorphism between $F[x]$ and $F'[x]$. □

Note 12.1.1

Since there is no difference between talking about φ and $\tilde{\varphi}$, we shall freely write $\tilde{\varphi}$ as φ without remorse.

Lemma 32 (Isomorphism Extension Lemma)

Let F and F' be fields, $\varphi : F[x] \to F'[x]$ be an isomorphism, $f(x) \in F[x]$ be irreducible, α be a root of $f(x)$ in an extension of F, and β be a

root of $f(x)$ be a root of $f(x)$ in an extension of F'. Then there exists an isomorphism $\psi : F(\alpha) \to F'(\beta)$ such that $\psi \restriction_F = \varphi$. Moreover, $\psi(\alpha) = \beta$.

Proof (Sketch)

Using the **First Isomorphism Theorem** to find ρ_1 and ρ_2, we have

$$F(\alpha) \xrightarrow{\rho_1} F[x]\Big/\langle f(x)\rangle \xrightarrow{\sigma} F'[x]\Big/\langle \varphi(f(x))\rangle \xrightarrow{\rho_2} F'(\beta),$$

[1] where $\sigma(\overline{g(x)}) = \overline{\varphi(g(x))}$. [2]

Then $\psi = \rho_2 \circ \sigma\rho_1 : F(\alpha) \to F'(\beta)$ is an isomorphism.

Let $a \in F$. Then

$$\psi(a) = \rho_2 \circ \sigma \circ \rho_1(a) = \rho_2 \circ \sigma(\bar{a}) = \rho_2(\overline{\varphi(a)}) = \varphi(a).$$

Also,

$$\psi(\alpha) = \rho_2 \circ \sigma \circ \rho_1(\alpha) = \rho_2 \circ \sigma(\bar{x}) = \rho_2(\overline{\varphi(x)}) = \rho_2(\bar{x}) = \beta. \qquad \square$$

[1]

Exercise 12.1.1
Prove that $\varphi(f(x))$ is irreducible.

[2]

Exercise 12.1.2
Prove that σ is an isomorphism.

It follows from induction that

Lemma 33 (Extended Isomorphism Extension Lemma)

Let F be a field, $f(x) \in F[x]$ non-constant, K a splitting field for $f(x)$ over F, F' a field, $\varphi : F \to F'$ an isomorphism, and K' a splitting field for $\varphi(f(x))$ over F'. Then there is an isomorphism $\psi : K \to K'$ such that $\psi \restriction_F = \varphi$.

Corollary 34 (Splitting Fields are Unique up to Isomorphism)

Let $f(x) \in F[x]$ be non-constant. If K and K' are splitting fields for $f(x)$ over F, then $K \cong K'$.

Proof

Consider $\varphi = id$ and use Lemma 33. □

12.2 Algebraic Closures

We talked about algebraicity, and it makes sense asking about where exactly 'upstairs' that we will be able to find all of the algebraic numbers over our given field. A lot of the machinery has been taken care of with the introduction of splitting fields.

Definition 16 (Algebraic Closures)

*A field $\bar{F}$ is an **algebraic closure** of a field F if*

1. *$\bar{F}/F$ is algebraic; and*
2. *every non-constant $f(x) \in F[x]$ splits over $\bar{F}$.*

Example 12.2.1

$\mathbb{C}$ is an algebraic closure for $\mathbb{R}$.

Example 12.2.2

$\mathbb{C}$ is **not** an algebraic closure for $\mathbb{Q}$.[3]

[3] Why?

Definition 17 (Algebraically Closed)

*A field F is **algebraically closed** if every non-constant $f(x) \in F[x]$ has a root in F.*

Remark 12.2.1

If F is algebraically closed, then every non-constant $f(x) \in F[x]$ splits over F.

Example 12.2.3

$\mathbb{C}$ is algebraically closed. 

13 Lecture 13 Feb 04th

13.1 Algebraic Closures (Continued)

This may seem obvious from the names (closure, closed?), but it is actually not immediately clear that algebraic closures are algebraically closed.

Proposition 35 (Algebraic Closures are Algebraically Closed)

If $\overline{F}$ is an algebraic closure for F, then $\overline{F}$ is algebraically closed.

Proof

Let $f(x) \in \overline{F}[x]$ be non-constant. Then by Kronecker's Theorem, $f(x)$ has a root α in some extension of $\overline{F}$. Since $\overline{F}(\alpha)/\overline{F}$ is algebraic and $\overline{F}/F$ is also algebraic, we have that $\overline{F}(\alpha)/F$ is algebraic. Thus α is a root of some $p(x) \in F[x]$. Since $\overline{F}$ is the algebraic closure of $\overline{F}$, $p(x)$ splits over $\overline{F}[x]$, and so it follows that $\alpha \in \overline{F}$. Therefore, $\overline{F}$ is algebraically closed. □

Theorem 36 (Every Field has an Algebraic Closure)

For every field F, there exists an algebraically closed field that contains F.

Note 13.1.1

Theorem 36 is an exercise in A5.

Theorem 37 (Smallest Algebraic Closure)

Let K be an algebraically closed field that contains F. The collection of elements in K which are algebraic over F is an algebraic closure of F.

Proof

Let

$$L := \{\alpha \in K \mid \alpha \text{ is algebraic over } F\}.$$

As given in the statement, we want to show that L is an algebraic closure of F.

It is clear that L/F, since every $\beta \in F$ is algebraic over F and is hence in L. Let $f(x) \in F[x]$ with $\deg f \geq 1$. Since $f(x)$ splits over K, we have

$$f(x) = u(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n),$$

where $u \in F^\times$ and $\alpha_i \in K$ for $i \in \{1,\dots,n\}$. Then since $f(\alpha_i) = 0$ for all i, it follows that each of the $\alpha_i \in L$. In other words, $f(x)$ splits over L. □

13.2 Cyclotimic Extensions

We look into a specific class of field extensions, which is rather important to us. Consider the following question:

> *What is the splitting field of the polynomial $f(x) = x^n - 1$ over $\mathbb{Q}$?*

The following definition should remind one of MATH 135.

Definition 18 (n^{th} Roots of Unity)

We call the roots of $x^n - 1$ (over $\mathbb{C}$) the n^{th} roots of unity.

Example 13.2.1

We can obtain all the n^{th} roots of unity using Euler's identity

$$\xi_n = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right),$$

which we label these roots as $1 = \xi_n^1, \xi_n^2, \xi_n^3, \ldots, \xi_n^{n-1}$.

Following the various results that we have proven in the last few lectures, we know that the splitting field of $x^n - 1$ over $\mathbb{Q}$ is therefore $\mathbb{Q}(\xi_n)$.

We can then ask ourselves what is the degree of $\mathbb{Q}(\xi_n)$ over $\mathbb{Q}$, i.e. what is $[\mathbb{Q}(\xi_n) : \mathbb{Q}]$?

If $n = p$ where p is prime, then since we may write

$$x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \ldots + x + 1),$$

by Item 4 in Example 7.1.3, we know that

$$\Phi_p(x) = x^{p-1} + \ldots + x + 1$$

is irreducible over $\mathbb{Q}$. So $\Phi_p(x)$ is the minimal polynomial for ξ_n over $\mathbb{Q}$.

It thus follows that $[\mathbb{Q}(\xi_p) : \mathbb{Q}] = p - 1$.

Example 13.2.2

We shall calculate $[\mathbb{Q}(\xi_6) : \mathbb{Q}]$. Note that

$$\xi_6 = \cos\left(\frac{2\pi}{6}\right) + i\sin\left(\frac{2\pi}{6}\right) = \frac{1}{2} + i\frac{\sqrt{3}}{2}.$$

Since $1, 2 \in \mathbb{Q}$, we have that $\mathbb{Q}(\xi_6) = \mathbb{Q}(i\sqrt{3})$. By 3-Eisenstein, the polynomial $x^2 + 3$ is irreducible and is a polynomial where $i\sqrt{3}$ is a root. Thus

$$[\mathbb{Q}(\xi_6) : \mathbb{Q}] = [\mathbb{Q}(i\sqrt{3}) : \mathbb{Q}] = \deg(x^2 + 3) = 2.$$

Remark 13.2.1

The n^{th} roots of unity form a cyclic group. A generator of this group is called a ***primitive n^{th} root of unity****.*

In other words, ξ_n^k is an primitive n^{th} root of unity iff $(\xi_n^k)^m \neq 1$ for $m = 1, 2, \ldots, n-1$.

From Group Theory, ξ_n^k is a primitive n^{th} root of unity iff $\gcd(n,k) = 1$. Thus, there are

$$\varphi(n) = |\{1 \leq k \leq n : \gcd(k,n) = 1\}|$$

primitive n^{th} root of unity[1].

[1] Explanation required.

Definition 19 (n^{th} Cyclotomic Polynomial)

For $n \geq 1$, the n^{th} cyclotomic polynomial is

$$\Phi_n(x) = \prod_{\substack{1 \leq k \leq n \\ \gcd(k,n)=1}} \left(x - e^{2\pi i \frac{k}{n}}\right) = (x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_{\varphi(n)}),$$

where the α_i's are the primitive n^{th} roots of unity.

Remark 13.2.2

Since $\Phi_n(x)$ has rational coefficients, we know that $\Phi_n(x) \in \mathbb{C}[x]$.

In fact, $\Phi_n(x)$ is the minimal polynomial for ξ_n over $\mathbb{Q}$, which then gives us that $[\mathbb{Q}(\xi_n) : \mathbb{Q}] = \varphi(n)$. However, we are not yet ready to show this.

Example 13.2.3

The following are n^{th} cyclotomic polynomials, where $n = 1, 2, 3$ and 4:

See the first 30 cyclotomic polynomials on Wikipedia.

- $\Phi_1(x) = x - 1$
- $\Phi_2(x) = \left(x - e^{2\pi i \frac{1}{2}}\right) = (x+1)$
- $\Phi_3(x) = \left(x + e^{2\pi i \frac{1}{3}}\right)\left(x - e^{2\pi i \frac{2}{3}}\right) = x^2 + x + 1$
- $\Phi_4(x) = (x+i)(x-i) = x^2 + 1$

Example 13.2.4

Let $n = p$ be prime. Then the p^{th} roots of unity are

$$1, \xi_p^2, \xi_p^3, \dots, \xi_p^{p-1}$$

and the primitives are

$$\zeta_p^2, \zeta_p^3, \ldots, \zeta_p^{p-1}.$$

Thus

$$x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \ldots + x^2 + x + 1) = (x-1)\Phi_p(x). \quad \text{📌}$$

A good question to ask here is:

> *Is there an easier way to compute $\Phi_n(x)$ for all n?*

14 Lecture 14 Feb 08th

14.1 Cyclotomic Extensions (Continued)

Remark 14.1.1

Note that $Z := \{z \in \mathbb{C} : z^n = 1\}$ *is a group. We may write*

$$\bigcup_{d|n} \left\{ \text{primitive } d^{th} \text{ roots of unity} \right\}.$$

Lemma 38 ($x^n - 1 = \prod_{d|n} \Phi_d(x)$)

We have

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

Example 14.1.1

$$\begin{aligned}\Phi_6(x) &= \frac{x^6 - 1}{\Phi_1(x)\Phi_2(x)\Phi_3(x)} \\ &= \frac{x^6 - 1}{(x-1)(x+1)(x^2+x+1)} = x^2 - x + 1.\end{aligned}$$

Proposition 39 (Cyclotomic Polynomials have Integer Coefficients)

For every $n \geq 1$, $\Phi_n(x) \in \mathbb{Z}[x]$.

Strategy

We shall use strong induction here.

Proof

We proceed by induction on n. If $n = 1$, then $\Phi_1(x) = x - 1 \in \mathbb{Z}[x]$.

Suppose the results holds for all $l < n$. By Lemma 38, we have

$$x^n - 1 = f(x)\Phi_n(x)$$

where

$$f(x) = \prod_{\substack{d|n \\ d<n}} \Phi_d(x).$$

By the induction hypothesis, $f(x) \in \mathbb{Z}[x]$. Let $F = \mathbb{Q}(\xi_n)$ so that $\Phi_n(x) \in F[x]$. By the division algorithm, $\exists! q(x), r(x) \in F[x]$ such that

$$x^n - 1 = f(x)q(x) + r(x).$$

Similarly, $\exists! \tilde{q}(x), \tilde{r}(x) \in \mathbb{Q}[x] \supset \mathbb{Z}[x]$ such that

$$x^n - 1 f(x)\tilde{q}(x) + \tilde{r}(x).$$

Since $\mathbb{Q} \subseteq F \subseteq \mathbb{C}$, by uniqueness[1],

$$\Phi_n(x) = q(x) = \tilde{q}(x) \in \mathbb{Q}[x].$$

It follows by Gauss' Lemnma that $\Phi_n(x) \in \mathbb{Z}[x]$. □

[1] This part should be thought of in the following way: we know that there is some $q(x) \in F[x]$, which is an extension of $\mathbb{Q}[x]$, and we also found that there is some $\tilde{q}(x) \in \mathbb{Q}[x]$, and so uniqueness tells us that the two must be the same.

Theorem 40 (Cyclotomic Polynomials are Irreducible over $\mathbb{Q}$)

For $n \geq 1$, $\Phi_n(x)$ is irreducible over $\mathbb{Q}$.

The proof for Theorem 40 is provided over two separate lectures, in particular it is provided at the end of this lecture and the beginning of Lecture 16. For sanity, the entire proof will be provided here.

Proof

Let $g(x) \in \mathbb{Q}[x]$ be a minimal polynomial for ξ_n. It suffices for us to show that $\Phi_n(x) \mid g(x)$. To that end, we can show that every root of $\Phi_n(x)$ is a root of $g(x)$ (in $\mathbb{C}$).

Let α be a root of $\Phi_n(x)$. Then by Definition 19, $\alpha = \xi_n^k$ for some $k \in \{1, \ldots, n-1\}$ such that $\gcd(k, n) = 1$. Then let $k = p_1 p_2 \ldots p_N$, where each p_i is a prime and $p_i \nmid n$ [2].

Strategy

We will show that $\Phi_n(x)$ is a minimal polynomial. If $g(x) \in \mathbb{Q}[x]$ is a minimal polynomial for ξ_n, then since ξ_n is also a root of $\Phi_n(x)$, we must have $g(x) \mid \Phi_n(x)$. So to show that $g(x)$ is actually $\Phi_n(x)$, it suffices to show that $\Phi_n(x) \mid g(x)$.

[2] Note that this must be the case since $\gcd(k, n) = 1$.

Thus, the statement which we wish to prove becomes the following: $\zeta_n^{p_1}, \zeta_n^{p_1 p_2}, \ldots, \zeta_n^{p_1 p_2 \cdots p_N} = \alpha$ are roots of $g(x)$.

To prove the above, it suffices for us to show that if $\xi \in \mathbb{C}$ is a root of $g(x)$, then ξ^p, where p is prime and $p \nmid n$, is also a root of $g(x)$.

Suppose not 😨, i.e. that $g(\xi) = 0$ but $g(\xi^p) \neq 0$, where p is prime and $p \nmid n$. Now since $g(x) \mid \Phi_n(x)$, we have $\Phi_n(\xi) = 0$. Since $p \nmid n$, it follows that ξ^p is also a primitive n^{th} root of unity, i.e. $\Phi_n(\xi_n^p) = 0$. Now since $g(x) \mid \Phi_n(x)$, $\exists h(x) \in \mathbb{Q}[x]$ such that $\Phi_n(x) = g(x)h(x)$. By Gauss, WMA $h(x) \in \mathbb{Z}[x]$. Since $\mathbb{Z}[x$ is an integral domain, $\Phi_n(\xi^p) = 0$ and $g(\xi^p) \neq 0 \implies h(\xi^p) = 0$.

Let $f(x) = h(x^p) \in \mathbb{Z}[x]$. Then $f(\xi) = 0$. Moreover, we have $g(x) \mid f(x)$ in $\mathbb{Q}[x]$. Thus $f(x) = g(x)k(x)$ for some $k(x) \in \mathbb{Z}[x]$ (again, through Gauss).

Suppose $h(x) = \sum b_j x^j$, which then implies that $f(x) = \sum b_j x^{pj}$. Consider $\bar{f}(x) \in \mathbb{Z}_p[x]$, i.e.

$$\bar{f}(x) = \sum \bar{b}_j x^{pj}, \quad \bar{b}_j \equiv b_j \mod p.$$

Then

$$\begin{aligned} \bar{f}(x) &= \sum \bar{b}_j^p x^{pj} \quad \because \textbf{Fermat's Little Theorem} \\ &= \left(\sum \bar{b}_j x^j\right)^p \quad \because \textbf{Freshman's Dream} \\ &= \left(\bar{h}(x)\right)^p. \end{aligned}$$

It follows that

$$\left(\bar{h}(x)\right)^p = \bar{f}(x) = \bar{g}(x)\bar{k}(x) \in \mathbb{Z}_p[x].$$

Now let $\bar{l}(x)$ be an irreducible factor of $\bar{g}(x)$ over $\mathbb{Z}_p[x]$ [3]. Since $\bar{l}(x) \mid \bar{h}(x)^p$, we have that $\bar{l}(x) \mid \bar{h}(x)$ [4].

On the other hand, in $\mathbb{Z}_p[x]$, we have that $\bar{\Phi}_n(x) = \bar{g}(x)\bar{h}(x)$. It follows that $\bar{l}(x)^2 \mid \bar{\Phi}_n(x)$ [5]. Since $\bar{\Phi}_n(x) \mid x^n - 1$, we have that

$$x^n - 1 = \bar{l}(x)^2 \bar{q}(x) \in \mathbb{Z}_p[x].$$

[3] Note that this $\bar{l}(x)$ may be $\bar{g}(x)$ itself if $\bar{g}(x)$ is still irreducible over $\mathbb{Z}_p[x]$.
[4] **Why?**
[5] **Why?**

By **taking derivatives** on both sides, we have

$$\begin{aligned}\bar{n}x^{n-1} &= 2\bar{l}(x)\bar{l}'(x)\bar{q}(x) + \bar{l}(x)^2\bar{q}'(x)\\ &= \bar{l}(x)[\bullet\bullet\bullet] \in \mathbb{Z}_p[x],\end{aligned}$$

where $\bullet\bullet\bullet$ is an irrelevant factor. Since $\bar{n} \neq 0$, we have that the only root of LHS is $\bar{0}$, and so the only root of $\bar{l}(x)$ is some extension of $\mathbb{Z}_p$ is $\bar{0}$. Since $\bar{l}(x) \mid x^n - \bar{1}$, we have that $\bar{0}^n - \bar{1} = 0$ but that mean $0 = 1 \in \mathbb{Z}_p$, a contradiction.

Tracing back our long convoluted line of thought, we have that 😵 is not true, and so we must have $g(\xi^p) = 0$, which

$\Longrightarrow$ all the $\xi_n^{p_1}, \xi_n^{p_1 p_2}, \ldots, \alpha$ are all roots of $g(x)$;

$\Longrightarrow$ $\Phi_n(x) \mid g(x)$;

$\Longrightarrow$ $\Phi_n(x) = g(x)$,

which is what we want to show. □

☞ Corollary 41 (Cyclotomic Polynomials are Minimal Polynomials of Its Roots over $\mathbb{Q}$)

$\Phi_n(x)$ is the minimal polynomial for ξ_n over $\mathbb{Q}$. In particular, $[\mathbb{Q}(\xi_n) : \mathbb{Q}] = \varphi(n)$.

Example 14.1.2

Let $f(x) = x^5 - 3$. Describe the splitting field of $f(x)$ over $\mathbb{Q}$. We shall find a basis for this splitting field over $\mathbb{Q}$.

The roots of $f(x)$ are

$$\sqrt[5]{3},\ \xi_5\sqrt[5]{3}, \xi_5^2\sqrt[5]{3}, \xi_5^3\sqrt[5]{3}, \xi_5^4\sqrt[5]{3}.$$

It follows that the splitting field for f is $F = \mathbb{Q}(\sqrt[5]{3}, \xi_5)$. Note that since

$$\deg_{\mathbb{Q}}(\xi_5) = \varphi(5) = 4 \text{ and } \deg_{\mathbb{Q}}(\sqrt[5]{3}) = 5,$$

it follows from A4Q2 that

$$[\mathbb{Q}(\sqrt[5]{3}, \xi_5) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[5]{3}) : \mathbb{Q}][\mathbb{Q}(\xi_5) : \mathbb{Q}] = 4 \cdot 5 = 20.$$

Now a basis for $\mathbb{Q}(\xi_5)(\sqrt[5]{3})/\mathbb{Q}(\xi_5)$ is

$$\left\{1, \sqrt[5]{3}, \left(\sqrt[5]{3}\right)^2, \left(\sqrt[5]{3}\right)^3, \left(\sqrt[5]{3}\right)^4\right\},$$

while a basis for $\mathbb{Q}(\xi_5)/\mathbb{Q}$ is

$$\left\{1, \xi_5, \xi_5^2, \xi_5^3\right\}.$$

Following the Tower Theorem, a basis for the splitting field F is

$$\left\{\left(\sqrt[5]{3}\right)^i (\xi_5)^j \;\middle|\; 0 \le i \le 4, 0 \le j \le 3\right\}.$$

15 Lecture 15 Feb 11th

15.1 Finite Fields

Finite fields are very easy to work with and grasp. The nice thing about finite fields is that, up to isomorphism, there is only one field that has order prime to some power, which we shall show in this section.

Lemma 42 (Units of a Finite Field Form a Finite Cyclic Group)

Let F be a finite field. Then $G = F^\times$ is a finite cyclic group.

Proof

Since G is the set of units of F, we know that G is an abelian group by its construction, and it is finite since F is finite. Then, by the **Finite Abelian Group Structure**, $\exists n_1, \dots, n_m \in \mathbb{Z}$ such that

$$G \simeq \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \dots \times \mathbb{Z}_{n_m}, \tag{15.1}$$

and each n_i is a prime power. Let

$$N := n_1 n_2 \dots n_m \text{ and}$$
$$M := \operatorname{lcm}(n_1, \dots, n_m).$$

By construction, $M \leq N$. Now $\forall a \in G$, we have that a is a root of $x^M - 1 \in F[x]$ due to Equation (15.1)[1].

[1] a is of one of the orders $n_1, n_2, \dots n_m$, so it is a root of $x^M - 1$.

Note that $N = |G|$, and the polynomial $x^M - 1$ has at most M roots. Therefore, $N \leq M$. Thus we must have $N = M$, thus forcing the n_i's

to be coprimes, and so we have

$$G \simeq \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_m} = \mathbb{Z}_N. \qquad \square$$

Proposition 43 (Order of Finite Fields are Powers of Its Primal Characteristic)

Let F be a finite field. Then

1. $|F| = p^n$, *where p is the characteristic*[2] *of F and $n = [F : \mathbb{Z}_p]$.*
2. $F = \mathbb{Z}_p(\alpha)$ *for some α such that* $\deg_{\mathbb{Z}_p}(\alpha) = n$.

[2] Recall from PMATH 347 that the definition of the characteristic is the order of 1 under addition. We shall use $\mathrm{Char}(F)$ to mean the characteristic of the field F.

Proof

Let F be a finite field with characteristic p. Then $\mathbb{Z}_p$ is a prime subfield of F, and in particular $F/\mathbb{Z}_p$. Let $n = [F : \mathbb{Z}_p]$. By Lemma 42, let $\alpha \in G = F^\times$ be such that $G = \langle \alpha \rangle$. By adding a unit of F to $\mathbb{Z}_p$, since $\mathbb{Z}_p$ is a prime subfield, we have that $\mathbb{Z}_p(\alpha) = F$.

Now since $n = [F : \mathbb{Z}_p]$, we have that

$$F = \mathrm{span}_{\mathbb{Z}_p}\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}.$$

It follows that $|F| = p^n$. $\square$

Theorem 44 (Finite Fields as Splitting Fields)

Let p be a prime and $n \in \mathbb{N}$. Then F is a finite field of order p^n iff F is the splitting field of $f(x) = x^{p^n} - x$ over $\mathbb{Z}_p[x]$.

Theorem 44 is the important theorem that tells us that there is only one finite field for every p^n up to isomorphism, and this follows from the uniqueness of splitting fields.

Proof

Suppose $|F| = p^n$. By Lagrange[3], $a^{p^n-1} - 1 = 0$ for every $a \in F^\times$.

[3] Is it really Lagrange?

Then in particular,

$$a(a^{p^n} - 1) = a^{p^n} - a = 0.$$

It follows that every $a \in F$ is a root of $x^{p^n} - x$.

Since $x^{p^n} - x$ has at most p^n roots, F must thus contain al roots of $x^{p^n} - x$, and so $x^{p^n} - x$ splits over $F[x]$. Any proper subfield of F would not have enough elements to be a splitting field for $x^{p^n} - x$. Thus F is a splitting field of $x^{p^n} - x$.

For the $\Longleftarrow$ direction, let F be the splitting field of $f(x) = x^{p^n} - x$. Let

$$K = \{\alpha \in F : f(\alpha) = 0\}.$$

Exercise 15.1.1

K is a field.

Then $K \leq F$. However, we also have that $F \leq K$, since all roots of f are in F since F is a splitting field, and f also splits over K.

Also, note that $f'(x) = -1$ since $\operatorname{Char} F = p$, and so f has no repeated roots since it is a decreasing function. □

Solution (to the ex. in the proof)
For $\alpha, \beta \in K$, we have that

$$\alpha^{p^n} - \alpha = 0 \text{ and } \beta^{p^n} - \beta = 0.$$

It then follows by the Freshman's Dream that

$$\left(\alpha^{p^n} + \beta^{p^n}\right) - \alpha - \beta = 0$$
$$\Longrightarrow$$
$$(\alpha + \beta)^{p^n} - (\alpha + \beta) = 0.$$

16 Lecture 16 Feb 13th

16.1 Finite Fields (Continued)

By Lemma 42, Proposition 43 and Theorem 44, we have the following result.

Since I moved the 'second half' of the proof of Theorem 40 over to Chapter 14, not too much content is left here.

Theorem 45 (Classification of Finite Fields)

For any prime p and $n \in \mathbb{N}$, we have

- *there exists a field F such that $|F| = p^n$; and*
- *any 2 fields of order p^n are isomorphic to one another.*

Note 16.1.1 (Notation)

We denote the field of order p^n by $\mathbb{F}_{p^n}$, i.e.

$$\mathbb{F}_{p^n} := \left\{ x \;\middle|\; f(x) = x^{p^n} - x = 0 \right\}.$$

In the next lecture, we shall prove the following theorem.

Theorem (Subfields of Finite Fields)

If E is a subfield of $\mathbb{F}_{p^n}$, then $E \simeq \mathbb{F}_{p^r}$, where $r \mid n$. Moreover, if $r \mid n$, then $\mathbb{F}_{p^n}$ has a unique[1] subfield of order p^r.

[1] This is truly unique, not unique up to isomorphism, which is **rare**.

The above theorem gives us the following example.

Example 16.1.1

Given the finite field $\mathbb{F}_{2^{12}}$, we know that the divisors of 12 are

$$1, 2, 3, 4, 6, 12.$$

By the above theorem, we have the following **lattice structure**.

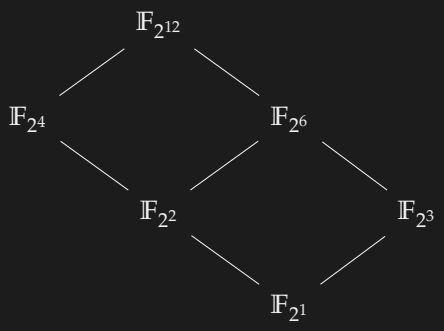

Figure 16.1: Lattice of $\mathbb{F}_{2^{12}}$

Part III

Galois Theory

17 Lecture 17 Feb 15th

17.1 Finite Fields (Continued 2)

We shall now prove the last theorem that we stated.

Theorem 46 (Subfields of Finite Fields)

If E is a subfield of $\mathbb{F}_{p^n}$, then $E \simeq \mathbb{F}_{p^r}$, where $r \mid n$. Moreover, if $r \mid n$, then $\mathbb{F}_{p^n}$ has a unique[1] *subfield of order p^r.*

[1] This is truly unique, not unique up to isomorphism, which is **rare**.

Proof

Part 1 Let $E < \mathbb{F}_{p^n}$. By Proposition 43 and the Tower Theorem, we have

$$n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : E][E : \mathbb{F}_p].$$

Then by letting $r = [E : \mathbb{F}_p]$, we have that $r \mid n$ and $|E| = p^r$.

Part 2 Suppose $r \mid n$, i.e. $\exists k \in \mathbb{Z}$ such that $n = rk$. Consider

$$\mathbb{F}_{p^n} = \left\{ \alpha \in \bar{\mathbb{F}}_p \;\middle|\; \alpha^{p^{rk}} - \alpha = 0 \right\},$$

[2]which we see is the splitting field of $x^{p^n} - x$, i.e. it is the set of roots of $x^{p^n} - x$. Since $r \mid n$, we have

[2] Note that we consider the closure just so that we contain all the roots. **Should $\mathbb{F}_{p^n}$ not already have everything?**

$$p^n - 1 = (p^r - 1)(p^{n-r} + p^{n-2r} + \ldots + p^r + 1).$$

Then, let

$$\begin{aligned} E &:= \left\{ \alpha \in \overline{\mathbb{F}}_p \;\middle|\; \alpha^{p^r} - \alpha = 0 \right\} \\ &= \left\{ \alpha \in \overline{\mathbb{F}}_p \;\middle|\; \alpha^{p^r - 1} - 1 = 0 \right\} \cup \{0\} \\ &\subseteq \overline{\mathbb{F}}_{p^n}. \end{aligned}$$

Moreover, we have that $|E| = p^r$.

For uniqueness, suppose if there exists $K < \mathbb{F}_{p^n}$ with order p^r. Then $\forall \alpha \in K$,

$$\alpha^{p^r} - \alpha = 0 \implies \alpha \in E.$$

Thus $K = E$. □

17.2 Introduction to Galois Theory

Let $f(x) \in F[x]$ be non-constant, and $\alpha_1, \ldots, \alpha_n$ be the roots of $f(x)$ in its splitting field K. Our goal is to study these roots by permuting them under automorphisms of the splitting field K.

Definition 20 (Galois Group)

Let K/F. We define the Galois Group of K/F, by

$$\mathrm{Gal}(K/F) := \{\varphi \in \mathrm{Aut}(K) \mid \varphi \restriction_F = id\} \leq \mathrm{Aut}(K),$$

where $\mathrm{Aut}(K)$ is the group of automorphisms of K.

Lemma 47 (The Galois Group permutes roots)

Let K/F. If $\alpha \in K$ is a root of $f(x) \in F[x]$ and $\varphi \in \mathrm{Gal}(K/F)$, then $\varphi(\alpha)$ is also a root of $f(x)$.

Proof

Let $f(x) \in F[x]$. Then $f(x) = \sum a_i x^i$. Since α is a root, we have

$f(\alpha) = \sum a_i \alpha^i = 0$. Since φ is an automorphism, we must therefore have $0 = \varphi(0)$. Since $\varphi \in \mathrm{Gal}(K/F)$, we have that

$$0 = \varphi(0) = \varphi(\sum a_i \alpha^i) = \sum \varphi(a_i)\varphi(\alpha^i) \overset{(*)}{=} \sum a_i \varphi(\alpha)^i = f(\varphi(\alpha)),$$

where $(*)$ is since φ fixes F. □

Corollary 48 (Elements of the Galois Group permutes roots of the same minimal polynomial)

Let K/F. If $\alpha \in K$ is algebraic over F, and $\varphi \in \mathrm{Gal}(K/F)$, then $\varphi(\alpha)$ is algebraic over F, and α and $\varphi(\alpha)$ has the same minimal polynomial in $F[x]$.

Example 17.2.1

Let $F = \mathbb{Q}$ and $K = F(\sqrt{2})$. Then $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \mathrm{Aut}\,\mathbb{Q}(\sqrt{2})$ [3]. Note that the minimal polynomial of $\sqrt{2}$ is $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2}) \in K[x]$. Thus if $\varphi \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$, then $\varphi(\sqrt{2}) = \sqrt{2}$ or $-\sqrt{2}$ [4]. It follows that the only two maps in $\mathrm{Gal}(K/F)$ are

$$\varphi_1 : a + b\sqrt{2} \mapsto a + b\sqrt{2}$$
$$\varphi_2 : a + b\sqrt{2} \mapsto a - b\sqrt{2}.$$

Thus $\mathrm{Gal}(K/F) = \{\varphi_1, \varphi_2\} \simeq \mathbb{Z}_2$.

[3] **Why**? Is it cause there is very little room for us to wiggle around $\varphi\restriction_F = id$?

[4] Note that we must fix everything else, by definition of a Galois group.

18 Lecture 18 Feb 25th

18.1 Introduction to Galois Theory (Continued)

Example 18.1.1

Consider the Galois group $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$. Now the minimal polynomial for $\sqrt{2}$ and $\sqrt{3}$ are

$$x^2-2, \text{ and } x^2-3,$$

respectively. Then we can only have $\varphi(\sqrt{2}) = \pm\sqrt{2}$ and $\varphi(\sqrt{3}) = \pm\sqrt{3}$, i.e. So $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}) = \{\varphi_i : i = 1,2,3,4\}$. Note that $|\varphi_i| = 2$ for

	$\sqrt{2}$	$\sqrt{3}$
φ_1	$\sqrt{2}$	$\sqrt{3}$
φ_2	$\sqrt{2}$	$-\sqrt{3}$
φ_3	$-\sqrt{2}$	$\sqrt{3}$
φ_4	$-\sqrt{2}$	$-\sqrt{3}$

Table 18.1: All possible elements of $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$

$i = 2,3,4$. It follows that $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$ is abelian and has order 4. Therefore

$$\mathrm{Gal}\left(\mathbb{Q}(\sqrt{2},\sqrt{3})\,/_{\mathbb{Q}}\right) \simeq \mathbb{Z}\times\mathbb{Z}.$$

Example 18.1.2

Consider $G = \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$. Let $\varphi \in G$. Since $\varphi(\sqrt[3]{2})$ is a root of x^3-2, we must have that

$$\varphi(\sqrt[3]{2}) \in \left\{\sqrt[3]{2},\ \sqrt[3]{2}\zeta_3,\ \sqrt[3]{2}\zeta_3^2\right\}.$$

However, $\sqrt[3]{2}\zeta_3,\ \sqrt[3]{2}\zeta_3^2 \notin \mathbb{Q}(\sqrt[3]{2})$. Therefore we must have $\varphi(\sqrt[3]{2}) = \sqrt[3]{2}$, i.e. $\varphi = id$. It follows that $G = \{1\}$.

Notice that in Example 18.1.2, the field where the roots lie in is important; we see that the Galois group ended up being the trivial group because the other roots of the minimal polynomial of $\sqrt[3]{2}$ live in a higher extension.

18.2 *The Galois Group as a Permutation Group*

Let F be a field, $f(x) \in F[x]$, $\deg f = n \geq 1$, and K a splitting field of $f(x)$ over F. Let $\alpha_1, \ldots, \alpha_n \in K$ be the roots of $f(x)$, and let $G = \mathrm{Gal}(K/F)$. From the last few examples, we notice that for any $\varphi \in G$, $\varphi(\alpha_i) = \alpha_j$.

In this section, we will show that G is actually a **permutation group** of the roots, as a subgroup of S_n in the case of permuting the roots of $f(x)$, the degree n polynomial.

In fact, more is true, but we shall see that down the road.

From the last two examples, one cannot help but notice a possible problem:

> *what if there are repeated roots?*

If there are, indeed, repeated roots, say $\alpha_1 = \alpha_2$ among the roots $\alpha_1, \alpha_2, \alpha_3, \alpha_4$, where $\alpha_4 \neq \alpha_3 \neq \alpha_1 \neq \alpha_4$, then the identity element would be indistinguishable from φ that is defined as

$$\varphi(\alpha_1) = \alpha_2,\ \varphi(\alpha_2) = \alpha_1,\ \varphi(\alpha_3) = \alpha_3,\ \varphi(\alpha_4) = \alpha_4.$$

So it suffices for us to consider for the case where $f(x)$ does not have multiple roots of the same value, i.e. the **multiplicity** of all roots is 1. Such polynomials are called **separable** polynomials.

Definition 21 (Separable Polynomials)

*A polynomial $f(x) \in F[x]$ is said to be **separable** if all of its roots have multiplicity* 1.

Let $f(x) \in F[x]$ be separable with $\deg f = n \geq 1$, and suppose K is the splitting field of $f(x)$ over F. Let $\alpha_1, \ldots, \alpha_n$ be the roots of f in K. From our discussion above, we want to show that $\mathrm{Gal}(K/F) \simeq P \leq S_n$. In

other words, we want to see that given $\varphi \in \mathrm{Gal}(K/F)$, $\exists \pi \in P \leq S_n$ such that $\varphi(\alpha_i) = \alpha_{\pi(i)}$.

Notation

Given $f(x) \in F[x]$, and K the splitting field of $f(x)$, we sometimes write

$$\mathrm{Gal}(f(x)) := \mathrm{Gal}(K/F).$$

In other words, when we write $\mathrm{Gal}(f(x))$, we are talking about the Galois group over the splitting field of $f(x)$ over F.

Example 18.2.1

Recall an earlier example of ours where $f(x) = (x^2-2)(x^2-3) \in \mathbb{Q}[x]$, where we showed that the Galois group $\mathrm{Gal}(f(x)) = \mathbb{Z}_2 \times \mathbb{Z}_2$. Let

$$\alpha_1 = \sqrt{2},\ \alpha_2 = -\sqrt{2},\ \alpha_3 = \sqrt{3},\ \alpha_4 = -\sqrt{3}.$$

Then

$$\mathrm{Gal}(f(x)) \simeq \{\varepsilon,\ (3\ 4),\ (1\ 2),\ (1\ 2)(3\ 4)\}.$$

Example 18.2.2

Let $x^2+1 \in \mathbb{Q}[x]$. Then [1]

[1] The adjoined elements are $\pm i$.

$$\mathrm{Gal}(x^2+1) \simeq \mathbb{Z}_2.$$

However, if we consider $x^2+1 \in \mathbb{Z}_2[x]$, then

$$\mathrm{Gal}(x^2+1) = \mathrm{Gal}((x+1)^2) = \{1\}.$$

The following is a quick corollary of from our discussion and observation.

Corollary 49 (The Galois Group completely captures all permutation of the roots)

Let F be a field, $f(x) \in F[x]$ a non-constant and irreducible, K a splitting

field of $f(x)$ over F. Then $\forall \alpha, \beta \in K$ such that $f(\alpha) = 0 = f(\beta)$, $\exists \varphi \in \mathrm{Gal}(K/F) = \mathrm{Gal}(f(x))$ such that $\varphi(\alpha) = \beta$.

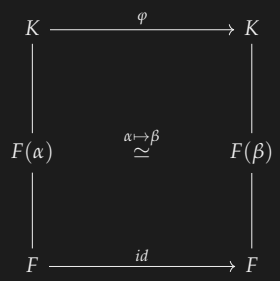

Figure 18.1: Constructing elements of the Galois Group

Proof

We shall use the Isomorphism Extension Lemma to prove this.

Consider the identity as our isomorphism $id : F \to F$. The Isomorphism Extension Lemma gives us the isomorphism that goes from $F(\alpha)$ to $F(\beta)$ by mapping α to β. We may thus define φ such that φ fixes F and $\varphi(\alpha) = \beta$, in K. □

Permutation groups that allows one to traverse all around the indices, such as the Galois group, have a special name.

Definition 22 (Transitive Subgroup)

*A subgroup $H \leq S_n$ is **transitive** if $\forall i, j \in \{1, \dots, n\}$, $\exists \pi \in H$ such that $\pi(i) = j$.*

Corollary 50 (The Galois Group of a Separable, Irreducible Polynomial is Transitive)

Let $f(x) \in F[x]$, with $\deg f = n \geq 1$, be separable and irreducible. Then $\mathrm{Gal}(f(x)) \simeq H \leq S_n$ that is transitive.

Example 18.2.3

Consider $G = \mathrm{Gal}(x^3 - 2)$ over $\mathbb{Q}[x]$.

Since $f(x) = x^3 - 2$ is irreducible (by 2-Eisenstein) and $\mathrm{Char}\,\mathbb{Q} = 0$, $f(x)$ is separable [2]. It follows from Corollary 50 that $G \simeq H \leq S_3$ transitive.

[2] See A5Q3(d).

Let $\alpha_1, \alpha_2, \alpha_3$ be the roots of $f(x)$. Let $X = \{\alpha_1, \alpha_2, \alpha_3\}$, and G act on X via $\varphi \cdot \alpha_i = \varphi(\alpha_i)$. By the Orbit-Stabilizer Theorem, we have

$$|G| = |\text{orb}(\alpha_1)| \cdot |\text{stab}(\alpha_1)| = 3 \cdot |\text{stab}(\alpha_1)|,$$

where we note that $|\text{orb}(\alpha_1)|$ since all the orbits of α_1 are exactly elements of X. It follows that $3 \mid |G|$. Since the only subgroups of S_3 that are divisible by 3 are A_3 and S_3, we either have

$$G \simeq A_3 \text{ or } G \simeq S_3.$$

We shall finish the rest of this example in the next lecture.

19 Lecture 19 Feb 27th

19.1 The Galois Group as a Permutation Group (Continued)

We shall continue with the last example of the last lecture.

Example 19.1.1

We considered $G = \mathrm{Gal}(x^3 - 2)$ over $\mathbb{Q}[x]$, and showed that we either have

$$G \simeq A_3 \text{ or } G \simeq S_3.$$

Recall that the roots of $f(x) = x^3 - 2$ are

$$\alpha_1 = \sqrt[3]{2},\ \alpha_2 = \alpha_1\zeta_3,\ \alpha_3 = \alpha_1\zeta_3^2.$$

Note that $f(x)$ is irreducible over $\mathbb{Q}(\zeta_3)$ [1]. By the Corollary 49, $\exists \varphi \in G$ such that we have the relation as shown in Figure 19.1.

[1] Well, none of the roots of f are in $\mathbb{Q}(\zeta_3)$, after all. Also, note that since $\alpha_1 \notin \mathbb{Q}(\zeta_3)$, f remains the minimal polynomial of α_1 over $\mathbb{Q}(\zeta_3)$, and so $\deg_{\mathbb{Q}(\zeta_3)}(\alpha_1) = 3$, but $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$.

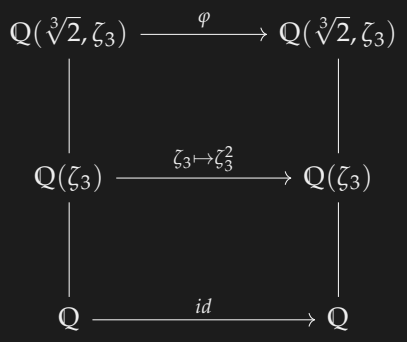

Figure 19.1: Corollary 49 in action

[2] Note that

[2] Note that $\zeta_3 \mapsto \zeta_3^2$ is a valid isomorphism, especially since they have the same minimal polynomial.

$$\varphi(\alpha_1) = \alpha_1$$
$$\varphi(\alpha_2) = \varphi(\alpha_1\zeta_3) = \alpha_1\zeta_3^2 = \alpha_3$$
$$\varphi(\alpha_3) = \varphi(\alpha_1\zeta_3^2) = \alpha_1\zeta_3 = \alpha_2$$

It thus follows that $\varphi \sim (2\ 3)$, a 2-cycle, in G. Thus φ is an element of order 2, which is an element that A_3 does not have. Thus $G \simeq S_3$.

From the above example, we notice the following helpful observation.

Remark 19.1.1

When computing $G = \mathrm{Gal}(K/F)$, it is often helpful to first know $|G|$.

Fortunately, in the finite dimensional world, $|G|$ has an upper bound.

Definition 23 (F-map)

*Let K/F and E/F. Any **homomorphism** $\varphi : K \to E$ which fixes F, i.e. $\varphi\restriction_F = id_F$, is called an F-map.*

Remark 19.1.2

Suppose K/F and E/F, and $\varphi : K \to E$ an F-map.

1. *Since $\ker\varphi \neq K$, we have $\ker\Phi = 0$ [3]. Thus φ is **injective**.*
2. *For any $\alpha \in F$, $v \in K$, $\varphi(av) = \varphi(a)\varphi(v) = a\varphi(v)$ since φ is a homomorphism. It follows that φ is a **linear transformation**.*
3. *Let $\varphi : K \to K$ be an F-map, and suppose K is a finite-dimensional F-vector space with $[K : F] < \infty$. Then φ is surjective.*

   It follows that $\varphi : K \to K$ ($[K : F] < \infty$) is an F-map $\iff$ $\varphi \in \mathrm{Gal}(K/F)$.

[3] Note that in finite fields, $\ker\varphi \in \{\{0\}, K\}$.

Lemma 51 (Number of Distinct F-maps)

Let K/F and E/F, and suppose K/F is a finite extension. The number of distinct F-maps from K to E is at most $[K : F]$.

Proof

We shall do induction on the number of generators of K/F, which is also $[K : F] = n$, which is what we can iterate on. When $n = 1$, we have $K = F(\alpha_1)$ and $\varphi : K \to E$ an F-map. Then the roots α_1 and $\varphi(\alpha_1)$ have the same minimal polynomial [4] over F. Thus, there are at most $[K : F]$-many choices for $\varphi(\alpha_1)$, meaning that there are at most $[K : F]$-many such F-maps.

[4] **Why?**

WTS that the number of F-maps is at most $[K : F] = [K : L][L : F]$. We can get $[L : F]$ from the **induction hypothesis** and $[K : L]$ from an argument similar to the base case.

Continuing with this inductive line of thought, suppose that the statement is true for $K = F(\alpha_1, \ldots, \alpha_n)$ for some $n > 1$. Now let

$$L = F(\alpha_1, \ldots, \alpha_{n-1}), \text{ so that } K = L(\alpha_n).$$

Let $\varphi : K \to E$ be an F-map. Note that $\varphi \restriction_L : F \to E$ is still an F-map. By the induction hypothesis, the number of choices for $\varphi \restriction_L$ is at most $[L : F]$. Since φ is completely determined by $\varphi \restriction_L$ and $\varphi(\alpha_n)$, there are, therefore, at most

$$[L : F][L(\alpha_n) : L] = [K : F]\text{-many}$$

choices for φ, following the Tower Theorem. □

The following corollary follows immediately from the realization that F-maps going from $K \to K$ are exactly the elements of the Galois group $\mathrm{Gal}(K/F)$.

Corollary 52 (Upper Bound for the Galois Group of Finite Extensions)

If K/F is finite, then

$$|\mathrm{Gal}(K/F)| \leq [K : F].$$

Warning

There are extensions K of a field F such that $\mathrm{Gal}(K/F) < [K : F]$.

1. *We saw in an earlier example that* $G = \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}) = \{1\}$, *but* $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, *and* $\sqrt[3]{2}\zeta_3$, $\sqrt[3]{2}\zeta_3^2 \notin \mathbb{Q}(\sqrt[3]{2})$. *In this case, the Galois group is too tiny.*

2. *Consider* $G = \mathrm{Gal}(\mathbb{Z}_2(x)/\mathbb{Z}_2(t^2))$. *Note that* $[\mathbb{Z}_2(x) : \mathbb{Z}_2(t^2)] = 2$, *since the minimal polynomial of* t *in* $\mathbb{Z}_2(t^2)[x]$ *is*

$$x^2 - t^2 = (x - t)^2 \in \mathbb{Z}_2(t)[x].$$

   Thus if $\varphi \in G$, *then it is necesssary that* $\varphi(t) = t$, *implying that* $G = \{1\}$.

   In this case, it is because t *is a root with multiplicity* > 1.

20 Lecture 20 Mar 01st

20.1 Galois Group of Separable Fields

So when exactly does $|\mathrm{Gal}(K/F)| = [K : F]$*?*

Definition 24 (Separable Elements and Separable Extensions)

Let K/F [1]*. We say that* $\alpha \in K$ *is* ***separable*** *if* α *is* ***algebraic*** *over* F *and its minimal polynomial is separable (over* F*)* [2]*.*

We say that the extension K/F *is* ***separable*** *if* K/F *is algebraic and* $\forall \alpha \in K$*,* α *is separable over* F*.*

[1] This need not be a finite extension.

[2] This also means that the root is unique.

Definition 25 (Perfect Fields)

We say that a field F *is* ***perfect*** *if every algebraic extension of* F *is separable.*

Remark 20.1.1

Definition 25 means that all polynomials over the field are separable, i.e. they do not have repeated roots.

Note 20.1.1

Recall from A5, we showed that given an irreducible $f(x) \in F[x]$*,*

$$f(x) \text{ is separable} \iff f'(x) \neq 0.$$

Proposition 53 (Separability and the Characteristic of a Field)

Let $f(x) \in F[x]$ be irreducible.

1. *If* $\operatorname{Char} F = 0$*, then $f(x)$ is separable.* [3]
2. *If* $\operatorname{Char} F = p$ *prime, then $f(x)$ is not separable iff $f(x) = g(x^p)$ for some $g(x) \in F[x]$.*

[3] This is proven in A5.

Proof

2. Let
$$f(x) \in a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$
Then $f(x)$ is not separable
$\iff f'(x) = 0$
$\iff na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \ldots + a_1 = 0$
$\iff ka_k = 0$ for $k \in \{1, \ldots, n\}$
$\iff ka_k = pm_k a_k$ where $m_k \in \mathbb{N}$, $k \in \{1, \ldots, n\}$ since either $p \mid k$ or $a_k = 0$
$\iff f(x) = a_n x^{m_n p} + a_{n-1}x^{m_{n-1}p} + \ldots + a_1 x^{m_1 p} + a_0$
$\iff f(x) = g(x^p)$ where
$$g(x) = a_n x^{m_n} + a_{n-1}x^{m_{n-1}} + \ldots + a_1 x^{m_1} + a_0. \qquad \square$$

Corollary 54 (Fields of Characteristic Zero are Perfect)

If $\operatorname{Char} F = 0$*, then F is perfect.*

Example 20.1.1

Note that in $\mathbb{Z}_2(t)/\mathbb{Z}_2(t^2)$, we have that
$$x^2 - t^2 = (x-t)^2,$$
i.e. t is a root with multiplicity 2. Thus $\mathbb{Z}_2(t^2)$ is not perfect.

Corollary 55 (Every Finite Field is Perfect)

Every finite field F is perfect.

Proof

Let F be finite with $\operatorname{Char} F = p > 0$ [4]. Suppose to the contrary that $\exists f(x) \in F[x]$ such that $f(x)$ is irreducible but not separable. Then $\exists g(x) \in F[x]$ such that $f(x) = g(x^p)$. In particular, we have

$$f(x) = a_n x^{pm_n} + a_{n-1} x^{pm_{n-1}} + \ldots + a_1 x^{pm_1} + a_0.$$

Now consider $\varphi : F \to F$ given by $\varphi(a) = a^p$. By the **Freshman's Dream**, φ is a homomorphism. It is clear that it is injective since if $a \neq b$, then $a^p \neq b^p$, for otherwise

$$0 = a^p - b^p = (a-b)^p \iff 0 = a - b \iff a = b.$$

Also, since F is finite, injectivity of φ guarantees that it is surjective. This means that $\forall a_k \in F$, $\exists b_k \in F$ such that

$$a_k = b_k^p = \varphi(b_k).$$

Then we have

$$\begin{aligned} f(x) &= b_n^p x^{pm_n} + b_{n-1}^p x^{pm_{n-1}} + \ldots + b_1^p x^{pm_1} + b_0^p \\ &= (b_n x^{m_n} + b_{n-1} x^{m_{n-1}} + \ldots + b_1 x^{m_1} + b_0)^p, \end{aligned}$$

again, by the **Freshman's Dream**. Therefore $f(x)$ is reducible, contradicting our assumption. □

Strategy

*Of course, we want to use Proposition 53. We can do so by supposing that $f(x)$ is irreducible but not separable, which then forces $f(x) = g(x^p)$. The important point here is to notice that in a finite field, all elements of the field will eventually cycle back as we add or multiply them. Then, by using the fact that $\operatorname{Char} F = p$ is prime, in particular by the **Freshman's Dream**, we can use **Frobenius's Homomorphism** $\varphi(a) = a^p$, and we end up showing that every element in F is some other element of F with power p. This will cause $f(x)$ to become reducible due to the Freshman's Dream.*

[4] Note that fields of characteristic 0 must be infinite, so this is a valid assumption.

Theorem 56 (Galois Group of a Splitting Field of a Separable Polynomial has Order the Degree of the Extension)

Let $f(x) \in F[x]$ be non-constant and separable. Let K be the splitting field of $f(x)$ over F. Then

$$|\operatorname{Gal}(K/F)| = |\operatorname{Gal}(f(x))| = [K : F].$$

Proof

We shall perform induction on $[K : F] = n$.

$n = 1$ We have

$$1 \leq |\mathrm{Gal}(K/F)| \leq [K : F] \leq 1,$$

since we always have $\varepsilon \in \mathrm{Gal}(K/F)$.

Proceeding inductively...

$n = k + 1$ Let $p(x) \in F[x]$ be an irreducible factor of $f(x)$ [5]. Note that $p(x)$ is also separable over F. Let

$$\alpha_1, \ldots, \alpha_m \in K$$

be the roots of $p(x)$, where $m = \deg p(x)$, and we note that $\alpha_i \neq \alpha_j$ for all $i \neq j$ since $p(x)$ is separable. Now since $[K : F] > 1$, wma $\alpha_1 \notin F$. Then consider $E = F(\alpha_1)$. Since $p(x)$ is irreducible in $F[x]$, it follows that $[E : F] = m$. Thus by the Tower Theorem, we have

$$[K : E] = \frac{[K : F]}{[E : F]} = \frac{n}{m} < n.$$

Note that we still have K as the splitting field of $f(x)$ over E. It follows from induction that

$$|\mathrm{Gal}(K/E)| = [K : E] = \frac{n}{m}. \tag{20.1}$$

Since $p(x)$ is irreducible, by the Isomorphism Extension Lemma, $\forall j$, $\exists \varphi_j \in \mathrm{Gal}(K/F)$ such that $\varphi_j(\alpha_1) = \alpha_j$. Since the roots are distinct, it follows that each of the φ_j's are distinct in $\mathrm{Gal}(K/F)$, and there are m-many such automorphisms.

Furthermore, we have that $\varphi_j^{-1}\varphi_i(\alpha_1) \neq \alpha_1 \in E$, and so $\varphi_j^{-1}\varphi_i \notin \mathrm{Gal}(K/E)$. This means that

$$\varphi_j \,\mathrm{Gal}(K/E) \neq \varphi_i \,\mathrm{Gal}(K/E),$$

[5] Note that it suffices for us to show for irreducible polynomials, since we can always factor a polynomial into irreducible terms.

and so we have that there must be

$$|\mathrm{Gal}(K/F)/\mathrm{Gal}(K/E)| \geq m.$$

By Lagrange, we have from Equation (20.1) that

$$|\mathrm{Gal}(K/F)| \geq m \cdot |\mathrm{Gal}(K/E)| = m \cdot \frac{n}{m} = n,$$

as desired. □

21 Lecture 21 Mar 04th

21.1 The Primitive Element Theorem

We shall now look at a rather 'simple' case of splitting fields of separable polynomials.

Definition 26 (Simple Extension and Primitive Elements)

*We say that K/F is **simple** if $\exists \alpha \in K$ such that $K = F(\alpha)$. We call α a **primitive element** for K/F.*

Theorem 57 (Primitive Element Theorem)

If K/F is finite and separable, then K/F is simple.

This is an important result to us, since it would imply the following.

Corollary 58 (Finite Extensions of Perfect Fields are Simple)

If F is perfect and K/F is finite, then K/F is simple.

Example 21.1.1

Fields of characteristic 0 and finite fields have simple extensions.

You may want to look at Analysis of the proof for the Primitive Element Theorem first before diving into the proof for Theorem 57. The proof provided in class makes the proof look as if it is a struck of genius, but it is actually through some frolicking around with finding out what we need, that one can realize why we chose to pick such a specifically defined S.

Proof (Theorem 57)

F is finite Then K is necessarily finite since it is a finite extension, and thus $K^\times = \langle \alpha \rangle$ for some $\alpha \in K$. Hence $K = F(\alpha)$.

Strategy

Note that Theorem 57 does not assume if F is finite or infinite, and so we must deal with either cases separately.

F is infinite Since K/F is finite, we may assume

$$K = F(\pi_1, \dots, \pi_n)$$

for some $\pi_i \in K$. It suffices for us to show that $\forall \alpha, \beta \in K$, $\exists \gamma \in K$ such that such that

$$K = F(\alpha, \beta) = F(\gamma),$$

since our desired result will simply follow by arguing repeatedly. Let $p(x)$ and $q(x)$ be the minimal polynomials of α and β, respectively, over F.

Now let L be the splitting field of $p(x)q(x)$ over K. Let the roots of $p(x)$ be

$$\alpha = \alpha_1, \alpha_2, \dots, \alpha_n,$$

and the roots of $q(x)$ be

$$\beta = \beta_1, \beta_2, \dots, \beta_m.$$

By separability, $\alpha_i \neq \alpha_j$ and $\beta_i \neq \beta_j$ for all $i \neq j$. Now let [1]

$$S := \left\{ \frac{\alpha_i - \alpha_1}{\beta_1 - \beta_j} \;\middle|\; 1 < i \leq n, 1 < j \leq m \right\}.$$

[1] Note that had we wanted to start with $\gamma = \beta + u\alpha$, we would have declared S with elements like $\frac{\beta_j - \beta_1}{\alpha_1 - \alpha_i}$.

Since S is finite while F is infinite, $\exists u \in F^\times$ such that $u \notin S$. Let $\gamma = \alpha + u\beta$.

Claim: $F(\alpha, \beta) = F(\gamma)$ Clearly, $F(\gamma) \subseteq F(\alpha, \beta)$ since $\gamma \in F(\alpha, \beta)$. Let $h(x)$ be the minimal polynomial of β over $F(\gamma)$. Since $q(\beta) = 0$, we have that $h(x) \mid q(x)$, and consequently if $h(\,\blacksquare\,) = 0$, then $\blacksquare = \beta_j$ for some $j \in \{1, \dots, m\}$.

Now let $k(x) = p(\gamma - ux) \in F(\gamma)[x]$. Notice that

$$k(\beta) = p(\gamma - u\beta) = p(\alpha) = 0.$$

Thus $h(x) \mid k(x)$. Notice that for $j > 1$, we have

$$\begin{aligned} k(\beta_j) = 0 &\iff p(\gamma - u\beta_j) = 0 \\ &\iff \gamma - u\beta_j = \alpha_i \text{ for some } i \\ &\iff \alpha_1 + u\beta_1 - u\beta_j = \alpha_i \\ &\iff u = \frac{\alpha_i - \alpha_1}{\beta_1 - \beta_j} \in S. \end{aligned}$$

Thus we know that for these j's, $k(\beta_j) \neq 0$ since we chose $u \notin S$.

It follows that $h(\beta_j) \neq 0$ for $j > 1$, and so $h(x) = x - \beta \in F(\gamma)[x]$, implying that $\beta \in F(\gamma)$. Using the same argument, we can show that $\alpha \in F(\gamma)$. This completes the proof, □

Strategy (Analysis of the proof for the Primitive Element Theorem) *If we want $F(\alpha, \beta) = F(\gamma)$ for some γ, one naive choice is to go with $\gamma = \alpha + u\beta$ for some $u \in F^\times$ and hope that this will force $\alpha, \beta \in F(\gamma)$. The argument is similar for either α or β (by switching variables), so let's think about only one of them. Now $q(x)$ is not necessarily a minimal polynomial of β over $F(\gamma)$, so let's make use of that.*

This is indeed a very profound result, making use of relatively simple notions such as minimal polynomials and splitting fields, and then proving for us a theorem that helps us narrow down the choice of the algebraic number to a single number that extends the base field to the extension.

If $\beta \in F(\gamma)$, then we must have $x - \beta \mid q(x)$. So let's consider the minimal polynomial $h(x)$ of β in $F(\gamma)$, which would divide $q(x)$. Of course, ideally, we want $h(x) = x - \beta$. Then let's suppose that $h(x)$ has some root other than β.

Then in the splitting field of $q(x)$, where $h(x)$ must then also split, since $q(x)$ is separable, we have that $h(x)$ must therefore be able to split into linear terms, where each linear term has a root of $q(x)$ as its constant value. In other words, all roots of $h(x)$ are roots of $q(x)$.

Then we notice another possible polynomial that such an $h(x)$ can divide: we know that $\alpha = \gamma - u\beta$, and α is a root of $p(x)$. Then if we let $k(x) = p(\gamma - ux)$, we have

$$k(\beta) = p(\gamma - u\beta) = p(\alpha) = 0.$$

So $h(x) \mid k(x)$. Now since all the roots of $h(x)$ are roots of $q(x)$, these roots must also be roots of $k(x)$. Let these other roots of $q(x)$ be labelled β_j's.

Then picking $\beta_j \neq \beta$, we have

$$k(\beta_j) = 0 \iff p(\gamma - u\beta_j) = 0.$$

We already know what the roots of $p(x)$ are so let's label those as α_i. Then

$$\gamma - u\beta_j = \alpha_i.$$

Note that $\alpha_i \neq \alpha$ since the roots are unique. Following that,

$$\alpha + u\beta - u\beta_j = \alpha_i,$$

which then

$$u = \frac{\alpha_i - \alpha}{\beta - \beta_j}. \tag{21.1}$$

We notice that there are only finitely many such u's in $F^\times$ since there are only as many as the roots α_i's and β_j's can allow. However, $F^\times$ is infinite by our assumption, i.e. there are always units of F that cannot be expressed as in Equation (21.1).

So by picking a $u \in F^\times$ that is not determined by Equation (21.1), we rule out the possibility that $k(x)$ has these other β_j's as roots, and hence forcing $h(x)$ to be what we want: that is $h(x) = x - \beta$. Thus our job is done for showing that $\beta \in F(\gamma)$!

We can then apply the same argument to showing that $\alpha \in F(\gamma)$, by letting $\gamma = \beta + u'\alpha$ by choosing u' in a similar fashion as above. In this case, we would have to extend our working field to the splitting field of $p(x)$.

Then to put the two together, we could have then started working with an extension where both $p(x)$ and $q(x)$ splits, and the splitting field of $p(x)q(x)$ is exactly where we should be working in.

22 Lecture 22 Mar 06th

22.1 Normal Extensions

Note 22.1.1

Given $f(x) \in F[x]$ irreducible, K the splitting field of $f(x)$ over F, $\alpha, \beta \in K$ the roots of $f(x)$, the Isomorphism Extension Lemma [1] *tells us that $\exists \varphi \in \mathrm{Gal}(K/F)$ such that $\varphi(\alpha) = \beta$.*

[1] See also Corollary 49.

There is a slightly more general result which we shall use today, whose proof shall be left as an exercise.

Exercise 22.1.1

Let $f(x) \in F[x]$ be non-constant, K the splitting field of $f(x)$ over F, and $\alpha, \beta \in K$ have the same minimal polynomial in $F[x]$. Then $\exists \varphi \in \mathrm{Gal}(K/F)$ such that $\varphi(\alpha) = \beta$.

Example 22.1.1

Recall our 'favorite' example $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{1\}$, where we had that the other roots of $x^3 - 2$, which are $\sqrt[3]{2}\zeta_3$ and $\sqrt[3]{2}\zeta_3^2$, are not in $\mathbb{Q}(\sqrt[3]{2})$. Notice that $x^3 - 2$ does not split in $\mathbb{Q}(\sqrt[3]{2})$.

Definition 27 (Normal Extension)

Let $[K : F] < \infty$. We say that K/F is normal if K is the splitting field of some non-constant $f(x) \in F[x]$.

Definition 28 (*F*-conjugates)

Let $[K : F] < \infty$. Let $\alpha \in K$ with minimal polynomial $p(x) \in F[x]$. The roots of $p(x)$ in its splitting field are called the F-conjugates (or just conjugates) of α.

We have the following theorem that characterizes normality.

Theorem 59 (Normality Theorem)

Let $[K : F] < \infty$. TFAE:

1. *K/F is normal.*
2. *For all extensions L over K, if φ is an F-map from $L \to L$, then $\varphi \restriction_K \in \mathrm{Gal}(K/F)$.*
3. *If $\alpha \in K$, then all F-conjugates of α are also in K.*
4. *If $\alpha \in K$, then its minimal polynomial splits over K.*

Proof

It is clear that $(3) \implies (4)$.

$(1) \implies (2)$ Suppose K/F is normal. Then K is the splitting field of some non-constant $f(x) \in F[x]$. Let $\varphi : L \to L$ be an F-map.

Since $[K : F] < \infty$, wma

$$K = F(\alpha_1, \dots, \alpha_n), \quad \alpha_i \in K,\ f(\alpha_i) = 0.$$

Then $\forall i$, $\exists j$ such that $\varphi \restriction_K (\alpha_i) = \alpha_j \in K$, since φ is an F-map. We see that $\varphi \restriction_K \in \mathrm{Gal}(K/F)$ both fixes F and is an automorphism of K.

$(2) \implies (3)$ Let $\alpha \in K$ with minimal polynomial $f(x) \in F[x]$. Since K/F is finite, once again, let

$$K = F(\alpha_1, \dots, \alpha_n)$$

for $\alpha_i \in K$. For each i, let $h_i(x)$ be the minimal polynomial of α_i over F. Now define [2]

$$p(x) = f(x)h_1(x)h_2(x)\dots h_n(x).$$

Let L be the splitting field of $p(x)$ over F. By construction, $L/K/F$ is a tower of fields. Let $\beta \in L$ be a root of $f(x)$ [3]. By Exercise 22.1.1, $\exists \varphi \in \mathrm{Gal}(K/F)$ such that $\varphi(\alpha_i) = \beta$. Since φ is an F-map, our assumption tells us that $\varphi \restriction_K \in \mathrm{Gal}(K/F)$. Since $\alpha_i \in K$, we have that $\beta \in K$. This proves what is required.

[2] We want to consider such a polynomial because it will contain all of the α_i's and their conjugates, and we hope to see that the splitting field of $p(x)$, where we can then apply our assumption.

[3] i.e. we consider a conjugate of α_i, for one of the i's.

(4) $\implies$ (1) Suppose K/F is finite, and write

$$K = F(\alpha_1, \dots, \alpha_n)$$

for $\alpha_i \in K$. Let $h_i(x)$ be the minimal polynomial of α_i over F. Let $f(x) = \prod_{i=1}^{n} h_i(x)$. It follows from (3) that the splitting field of $f(x)$ over F is $F(\alpha_1, \dots, \alpha_n) = K$ since K contains all of the F-conjugates of each α_i. Thus K/F is normal. □

Example 22.1.2

As we've just seen in this lecture, $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal since $\sqrt[3]{2}\zeta_3 \notin \mathbb{Q}(\sqrt[3]{2})$ while $\sqrt[3]{2} \in \mathbb{Q}(\sqrt[3]{2})$.

Example 22.1.3

$\mathbb{F}_{p^n} = \mathbb{F}_p$ is normal since $\mathbb{F}_{p^n}$ is the splitting field of $x^{p^n} - x \in \mathbb{F}_p[x]$.

Example 22.1.4

Cyclotomic extensions $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ are normal since it is the splitting field of $\Phi_n(x)$.

Example 22.1.5 (★)

$\mathbb{Z}_p(t)/\mathbb{Z}(t^p)$ is normal since it is the splitting field of $x^p - t^p = (x-t)^p$.

This is an example of a normal extension that is **not separable**.

22.2 *Galois Extensions*

Definition 29 (Galois Extension)

Suppose $[K : F] < \infty$. *We say that* K/F *is* ***Galois*** *if* K/F *is normal and separable.*

23 Lecture 23 Mar 08th

23.1 Galois Extensions (Continued)

Definition 30 (Fixed Field)

Let K be a field. If $G \leq \mathrm{Aut}(K)$, the fixed field of G is defined as

$$\mathrm{Fix}(G) := \{a \in K \mid \varphi(a) = a,\ \varphi \in G\}.$$

Exercise 23.1.1

Check that $\mathrm{Fix}(G) \leq K$ is indeed a field.

Remark 23.1.1

The following is noteworthy:

$$\mathrm{Fix}(\mathrm{Gal}(K/F)) \supseteq F.$$

This follows immediately from the definition of a Galois group.

Example 23.1.1

Consider

$$f(x) = (x - \sqrt{2})^2(x + \sqrt{2})^2 = x^4 - 4^2 + 4.$$

Then there are $\varphi \neq \varepsilon \in G = \mathrm{Gal}(f(x))$ such that $\varphi(\sqrt{2}) = \sqrt{2}$ (and $\varphi(-\sqrt{2}) = \sqrt{2}$). In this case,

$$\mathrm{Fix}(G) \supsetneq F.$$

Theorem 60 (Characterization of Galois Extensions)

Suppose $[K : F] < \infty$. *TFAE:*

1. *K is the splitting field of a non-constant separable $f(x) \in F[x]$ over F.*
2. $|\mathrm{Gal}(K/F)| = [K : F]$.
3. $\mathrm{Fix}(\mathrm{Gal}(K/F)) = F$.
4. *K/F is Galois.*

Proof

(1) $\implies$ (2) See Theorem 56.

(2) $\implies$ (3) Suppose $|\mathrm{Gal}(K/F)| = [K : F]$. By our earlier remark, we have that $\mathrm{Fix}(\mathrm{Gal}(K/F)) \supseteq F$. So it suffices to show that $\mathrm{Fix}(\mathrm{Gal}(K/F)) \subseteq F$.

Let $E = \mathrm{Fix}(\mathrm{Gal}(K/F))$. Then we have a tower $K/E/F$. By the Tower Theorem,

$$[K : F] = [K : E][E : F].$$

It suffices to show that $[E : F] = 1$.

Now, note that we have $\mathrm{Gal}(K/E) \leq \mathrm{Gal}(K/F)$ [1]. By assumption, we have

$$|\mathrm{Gal}(K/E)| \leq |\mathrm{Gal}(K/F)| = [K : F].$$

Let $\alpha \in E$ and $\varphi \in \mathrm{Gal}(K/F)$. By the construction of E, we have that $\varphi(\alpha) = \alpha$. It follows that φ also fixes E, and so $\varphi \in \mathrm{Gal}(K/E)$. Thus $\mathrm{Gal}(K/F) \leq \mathrm{Gal}(K/E)$. Hence $\mathrm{Gal}(K/E) = \mathrm{Gal}(K/F)$.

This shows that

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

which implies that $[E : F] = 1$, as we desired.

(3) $\implies$ (4) Suppose $\mathrm{Fix}(\mathrm{Gal}(K/F)) = F$. Let $\alpha \in K$ with minimal polynomial $p(x)$ over F. WTS $p(x)$ splits over K with no repeated

[1] Note that the former fixes more things, and so there is less 'space' for the permutations to move around.

roots. Let $G = \mathrm{Gal}(K/F)$.

Consider [2]

$$\Delta = \{\varphi(\alpha) : \varphi \in G\} \subseteq K.$$

Let $\alpha_1, \ldots, \alpha_n \in \Delta$ be distinct, and wlog wma $\alpha = \alpha_1$. Now consider

$$h(x) = (x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_n) \in K[x].$$

Then in $K[x]$, we have that $h(x) \mid p(x)$, since all roots of $h(x)$ are roots of $p(x)$. Now for any $\varphi \in G$, we have that $\varphi(\alpha_i) = \alpha_j$, and so

$$\varphi(h(x)) = h(x),$$

which means $h(x) \in \mathrm{Fix}(G)[x] = F[x]$ by assumption. Since $p(x)$ is the minimal polynomial of α in $F[x]$, it follows that $p(x) \mid h(x)$ and so $p(x) = h(x)$, which splits over K and has no repeated roots, just as we wanted.

[2] Δ gives us all the roots of $p(x)$.

(4) $\implies$ (1) Suppose K/F is Galois [3]. Since $[K : F] < \infty$, let

$$K = F(\alpha_1, \ldots, \alpha_n),$$

where $\alpha_i \in K$. Let $q_i(x) \in F[x]$ be the minimal polynomial of each α_i. Let $p_1(x), \ldots, p_m(x)$ be the distinct $q_i(x)$'s.

Since K/F is separable, we know that the $q_i(x)$'s are separable and hence so are the $p_i(x)$'s. Let

$$f(x) = p_1(x)p_2(x)\ldots p_n(x) \in F[x].$$

By A6Q3(b), we have that $f(x)$ is separable over F in K. Also, K/F is normal since the splitting field of $f(x)$ over F is exactly K. □

[3] By definition, K/F is normal and separable, which means

- (**normal**) K is the splitting field of some non-constant $f(x) \in F[x]$; and
- (**separable**) for each $\alpha \in K$, the minimal polynomial $p(x)$ of α over F is separable in K.

So there is actually something to prove because we only know that K is the splitting field of some polynomial that may or may not be a minimal polynomial of any $\alpha \in K$, and K may not be the splitting field of any of the minimal polynomial of its elements.

Example 23.1.2

Let's look at our non-Galois extension of $\mathbb{Q}$, $\mathbb{Q}(\sqrt[3]{2})$. We observe that

$$\mathrm{Fix}(\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})) = \mathbb{Q}(\sqrt[3]{2}),$$

since $\sqrt[3]{2}$ fixes even $\sqrt[3]{2}$ itself.

Example 23.1.3

Let $\alpha = \sqrt{2+\sqrt{3}} \in \mathbb{C}$. Note that

$$\begin{aligned} \alpha^2 &= 2+\sqrt{3} \\ \alpha^2 - 2 &= \sqrt{3} \\ (\alpha^2-2)^2 &= 3 \\ \alpha^4 - 4\alpha^2 + 4 &= 3 \\ \alpha^4 - 4\alpha^2 + 1 &= 0 \end{aligned}$$

Consider the polynomial

$$f(x) = x^4 - 4x^2 + 1 \in \mathbb{Q}[x],$$

and α is a root of $f(x)$. Now consider the polynomial

$$g(y) = y^2 - 4y + 1.$$

Note that in $\mathbb{Z}_5$, under $\tilde{g}(y) = y^2 + y + 1$, we have

$$\begin{aligned} 0 \mapsto 1 \quad 1 \mapsto 3 \quad 2 \mapsto 2 \\ 3 \mapsto 3 \quad 4 \mapsto 1. \end{aligned}$$

By 🔥 Proposition 14, $\tilde{g}(y)$ is irreducible, and by Mod-5 irreducibility, $g(y)$ is irreducible. Thus $f(x)$ itself is irreducible. Since f is monic, it is the minimal polynomial of α.

Note that by construction, all the roots of $f(x)$ are

$$\pm\sqrt{2\pm\sqrt{3}}.$$

Thus $f(x)$ is separable. Note that

$$\sqrt{2+\sqrt{3}}\sqrt{2-\sqrt{3}} = 1,$$

and so $\sqrt{2-\sqrt{3}}$ is the inverse of $\sqrt{2+\sqrt{3}}$, and so it is necessarily in $\mathbb{Q}(\alpha)$. It follows that all the $\mathbb{Q}$-conjugates of α are in $\mathbb{Q}(\alpha)$. Thus $\mathbb{Q}(\alpha)/\mathbb{Q}$ is normal.

It follows that $\mathbb{Q}(\alpha)/\mathbb{Q}$ is a Galois extension.

By the characterization of Galois extensions, we have

$$|\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})| = [\mathbb{Q}(\alpha) : \mathbb{Q}] = 4.$$

Let $\beta = \sqrt{2-\sqrt{3}}$. By the note that $\alpha\beta = 1$, we have that the following table describes all the possible actions of G on the $\mathbb{Q}$-conjugates of α.

	α	$-\alpha$	β	$-\beta$	S_4
φ_1	α	$-\alpha$	β	$-\beta$	ε
φ_2	$-\alpha$	α	$-\beta$	β	$(1\,2)(3\,4)$
φ_3	β	$-\beta$	α	$-\alpha$	$(1\,3)(2\,4)$
φ_4	$-\beta$	β	$-\alpha$	α	$(1\,4)(2\,3)$

Table 23.1: Table of elements of $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$.

By Table 23.1, it follows that

$$G \simeq K_4 \simeq \mathbb{Z}_2 \times \mathbb{Z}_2.$$

24 Lecture 24 Mar 11th

24.1 Fundamental Theorem of Galois Theory

We shall first prove the following theorem, which will take away the bulk of the work required to prove the fundamental theorem later on.

Theorem 61 (Artin's Theorem)

Let K be a field, and $H \leq \mathrm{Aut}(K)$ a finite subgroup. Let $F = \mathrm{Fix}(H)$. Then

1. *K/F is Galois.*
2. *$\mathrm{Gal}(K/F) = H$.*
3. *$|H| = |\mathrm{Gal}(K/F)| = [K : F]$.*

Proof

First, note that since $F = \mathrm{Fix}(H)$, we have that $H \subseteq \mathrm{Gal}(K/F)$ since, in a rather dumb way of putting it, H only moves the elements in K that it can, and it cannot move the elements in F since F is exactly the elements that H cannot move.

Then we have one part of (3), i.e.

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

where the second inequality is because we do not know if K is the splitting field of some non-constant separable polynomial in $F[x]$.

Strategy

One sensible approach is to see how large is this extension. Since $[K : F] \leq |H|$ is what we want, let's go against that.

One may resort to try to use technique that were used lately, particularly, considering minimal polynomials of elements in K algebraic over F, and then try to get to the splitting field of the polynomial of the product of those unique minimal polynomials. This, however, is not helpful, for we would go up into an extension where there is more 'freedom', and so making it difficult to find a contradiction.

Observe that if $[K : F] \leq |H|$, then all of our results will follow. In particular, (3) would then be true. Then, $|\mathrm{Gal}(K/F)| = [K : F]$ implies that K/F is Galois by the characterization of Galois extensions. Also, since $H \subseteq \mathrm{Gal}(K/F)$, $|H| = |\mathrm{Gal}(K/F)|$ would give us (2).

Let $|H| = m$. Let $\beta_1, \ldots, \beta_n \in K^\times$, and suppose to the contrary that $n > m$.[1]

[1] It is logical to make the next step provided that one is being conscious of knowledge from linear algebra.

Claim $\{\beta_1, \ldots, \beta_n\}$ is linearly dependent on F.

Consider the system of linear equations

$$\varphi(\beta_1)x_1 + \varphi(\beta_2)x_2 + \ldots + \varphi(\beta_n)x_n = 0,$$

where we let φ range over H. Since $|H| = m$, we have m-many such linear equations. Notice that there are more variables than there are equations, and so we must have a non-trivial solution $(x_1, x_2, \ldots, x_n) \in K^n$.

Note that if $\psi \in H$, for any $\varphi \in H$, since $\psi \in H$ is a homomorphism we have

$$\begin{aligned}
&\varphi(\beta_1)\psi(x_1) + \varphi(\beta_2)\psi(x_2) + \ldots \varphi(\beta_n)\psi_n \\
&= \psi\left(\psi^{-1}\varphi(\beta_1)x_1 + \psi^{-1}\varphi(\beta_2)x_2 + \ldots \psi^{-1}\varphi(\beta_n)x_n\right) \\
&= \psi^{-1}(0) = 0,
\end{aligned}$$

where the second last equality is because the term in the parenthesis is one of the linear equations from before. It follows that $(\psi(x_1), \ldots, \psi(x_n)) \in K^n$ is also a non-trivial solution. From this, we know that there are m-many such non-trivial solutions.

[2] Let $(x_1, \ldots, x_n)$ be a non-trivial solution with a minimal number of non-zero entries [3]. Reordering if necessary, wma

[2] This is a non-trivial step. I can't seem to figure out how this can come by though.
[3] We want this guy to have as many zeroes as possible.

$$(x_1, \ldots, x_n) = (x_1, \ldots, x_r, 0, \ldots, 0),$$

where for $i = 1, 2, \ldots, r$, we have $x_i \neq 0$. Note that $r > 1$, for otherwise $\varphi(\beta_1)x_1 = 0 \implies x_1 = 0$, a contradiction. Notice that

$$\left(1, \frac{x_2}{x_1}, \frac{x_3}{x_1}, \ldots, \frac{x_n}{x_1}\right)$$

is also a solution. Thus wma $x_1 = 1$, i.e. we assume

$$(x_1, x_2, \ldots, x_r, 0, \ldots, 0) = (1, x_2, x_3, \ldots, x_r, 0, \ldots, 0). \tag{24.1}$$

Now, notice that if $x_2, x_3, \ldots, x_r \in F$, then we have

$$\beta_1 + \beta_2 x_2 + \ldots \beta_n x_n = 0,$$

then β_1 is dependent on the others, and that would complete the proof.

Sub-claim $x_2, x_3, \ldots, x_r \in F$. Suppose not, i.e. suppose $x_i \notin F$. Then since $F = \text{Fix}(H)$, we know that $\exists \psi \in H$ such that $\psi(x_i) \neq x_i$. Wlog, sps $x_i = x_2$. We know that

$$(1, \psi(x_2), \psi(x_3), \ldots, \psi(x_r), 0, \ldots, 0)$$

is also a non-trivial solution to the earlier system of equations. Then consider

$$\begin{aligned}&(1, x_2, \ldots, x_r) - (1, \psi(x_2), \psi(x_3), \ldots, \psi(x_r), 0, \ldots, 0)\\ &= (0, x_2 - \psi(x_2), 0, \ldots, 0),\end{aligned}$$

which is also a non-trivial solution to the system of equations. However, this contradicts the minimality of Equation (24.1). Thus $x_2, x_3, \ldots, x_r \in F$. This completes our proof. □

Definition 31 (Galois Correspondences)

Let K be an extension of F. Let $\mathcal{E}$ denote the set of intermediate subfields of K/F, i.e.

$$\mathcal{E} := \{E : F \subseteq E \subseteq F\},$$

and $\mathcal{H}$ denote the subgroups of $\text{Gal}(K/F)$*, i.e.*

$$\mathcal{H} := \{H : H \leq \text{Gal}(K/F)\}.$$

*We define the **Galois correspondences** by*

$$\text{Gal}(K/-) : \mathcal{E} \to \mathcal{H} \text{ as } E \mapsto \text{Gal}(K/E)$$

and

$$\text{Fix} : \mathcal{H} \to \mathcal{E} \text{ and } H \mapsto \text{Fix}\, H.$$

Note 24.1.1

Notice that $\text{Gal}(K/-)$ *bring subfields to subgroups, while* Fix *brings subgroups to subfields.*

---

25 Lecture 25 Mar 13th

25.1 Fundamental Theorem of Galois Theory (Continued)

Remark 25.1.1

The Galois correspondences are ***inclusion reversing****: notice that*

1. $E_1 \subseteq E_2 \in \mathcal{E} \implies \mathrm{Gal}(K/E_2) \subseteq \mathrm{Gal}(K/E_1)$ *since the later Galois group has less elements to fix.*
2. $H_1 \subseteq H_2 \in \mathcal{H} \implies \mathrm{Fix}\, H_1 \subseteq \mathrm{Fix}\, H_2$ *since H_2 has more elements, and so it will move more things around, making the fix smaller.*

Theorem 62 (Fundamental Theorem of Galois Theory)

Let K/F be a finite Galois extension. Then the Galois correspondences give an inclusion reversing bijection between $\mathcal{E}$ and $\mathcal{H}$, i.e.

1. *if $E \in \mathcal{E}$, then $\mathrm{Fix}(\mathrm{Gal}(K/E)) = E$. In particular, K/E is Galois;*
2. *if $H \in \mathcal{H}$, then $\mathrm{Gal}(K/\mathrm{Fix}\, H) = H$.*

Proof

1. Since K/F is normal and separable, by A7, we have that K/E is also normal and separable. Thus it follows from the characterization of Galois extensions that

$$\mathrm{Fix}(\mathrm{Gal}(K/E)) = E.$$

2. This is exactly Artin's Theorem! □

Corollary 63 (Relation between Index and Degree)

Let K/F be a finite Galois extension. If $H_1 \subseteq H_2 \in \mathcal{H}$, then

$$|H_2 : H_1| = [\operatorname{Fix} H_1 : \operatorname{Fix} H_2].$$

If $K/E_1/E_2/F$ is a tower of fields, then

$$[E_1 : E_2] = |\operatorname{Gal}(K/E_2) : \operatorname{Gal}(K/E_1)|.$$

Proof

Notice that by the Tower Theorem, we have

$$\begin{aligned}[\operatorname{Fix} H_1 : \operatorname{Fix} H_2] &= \frac{[K : \operatorname{Fix} H_2]}{[K : \operatorname{Fix} H_1]} \\ &= \frac{|\operatorname{Gal}(K/\operatorname{Fix} H_2)|}{|\operatorname{Gal}(K/\operatorname{Fix} H_1)|} \\ &= \frac{|H_2|}{|H_1|} = |H_2 : H_1|.\end{aligned}$$

On the other hand, we have

$$\begin{aligned}[E_1 : E_2] &= \frac{[K : E_1]}{[K : E_2]} \\ &= \frac{|\operatorname{Gal}(K/E_1)|}{|\operatorname{Gal}(K/E_2)|} \\ &= |\operatorname{Gal}(K/E_2) : \operatorname{Gal}(K/E_1)|.\end{aligned}$$ □

Figure 25.1 illustrates what the fundamental theorem does.

Note 25.1.1 (★)

Notice that the index of each of the subgroups with respect to the base group becomes the degree of which the fix of the subgroup extends the base field.

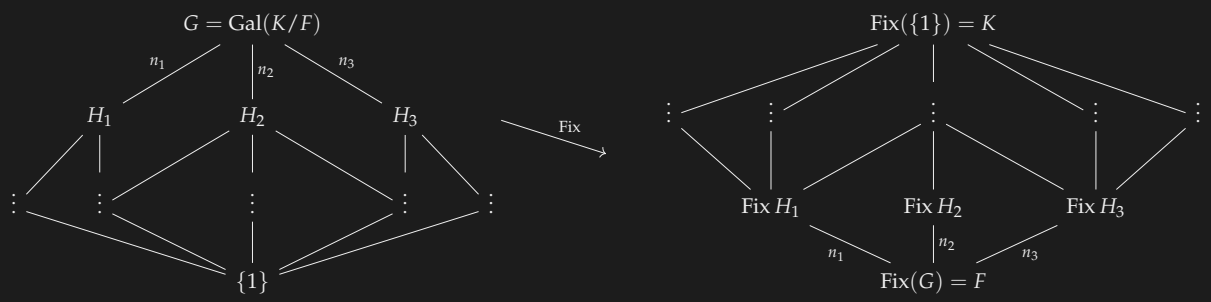

Figure 25.1: Visual Representation of the Fundamental Theorem of Galois Theory

The following is a typical problem for finding out about a Galois extension.

Example 25.1.1

Consider our 'favorite' extension

$$G = \mathrm{Gal}(\mathbb{Q}(\alpha, \zeta_3)/\mathbb{Q}) = \mathrm{Gal}(x^3 - 2),$$

where $\alpha = \sqrt[3]{2}$.

1. Prove that $\mathbb{Q}(\alpha, \zeta_3)/\mathbb{Q}$ is Galois.
2. Find $|G|$.
3. Find G.
4. Draw the subfield lattice.

Solution

1. Note that $\mathbb{Q}$ is perfect, so $x^3 - 2$ is separable. Also it is irreducible by 2-Eisenstein. And indeed, $\mathbb{Q}(\alpha, \zeta_3)$ is the splitting field of $x^3 - 2 \in \mathbb{Q}[x]$. Thus $\mathbb{Q}(\alpha, \zeta_3)/\mathbb{Q}$ is Galois.
2. Observe that
$$|G| = [\mathbb{Q}(\alpha, \zeta_3) : \mathbb{Q}] = 2 \cdot 3 = 6,$$
where the second equality follows from one of our assignment problems.
3. Since we have $G \leq S_3$ and $|G| = 6$, it follows that $G \simeq S_3$.
4. Since $G \simeq S_3$, we have the following **subgroup lattice**:

   One can indeed check that all 6 of the possible automorphisms on the

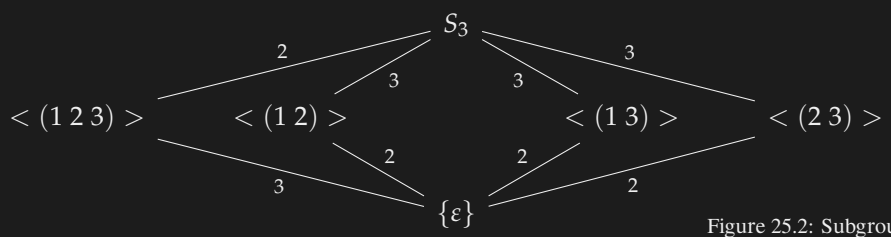

Figure 25.2: Subgroup Lattice of $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q})$

roots must occur, of which its result is shown in Table 25.1.

	α	$\alpha\zeta_3$	$\alpha\zeta_3^2$	S_3
φ_1	α	$\alpha\zeta_3$	$\alpha\zeta_3^2$	ε
φ_2	α	$\alpha\zeta_3^2$	$\alpha\zeta_3$	$(2\,3)$
φ_3	$\alpha\zeta_3^2$	α	$\alpha\zeta_3$	$(1\,2\,3)$
φ_4	$\alpha\zeta_3^2$	$\alpha\zeta_3$	α	$(1\,3)$
φ_5	$\alpha\zeta_3$	$\alpha\zeta_3^2$	α	$(1\,3\,2)$
φ_6	$\alpha\zeta_3$	α	$\alpha\zeta_3^2$	$(1\,2)$

Table 25.1: Structure of $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q})$

By the fundamental theorem, we have that the subfield lattice is as shown in Figure 25.3.

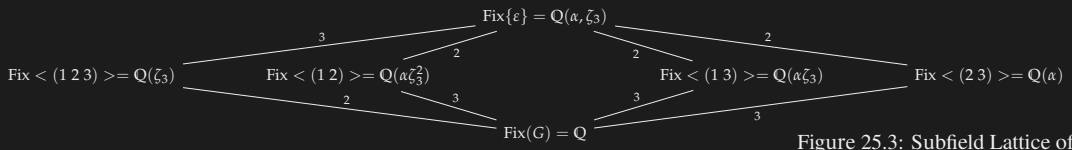

Figure 25.3: Subfield Lattice of $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q})$

26 Lecture 26 Mar 15th

26.1 Fundamental Theorem of Galois Theory (Continued 2)

Note 26.1.1

It is important to note that given a finite Galois extension, the Fundamental Theorem of Galois Theory tells us that there are only finitely many intermediary subfields up to isomorphism.

Proposition 64 (Other Subfields Through Group Normality)

Let K/F be a finite Galois extension. Let E be an intermediate subfield of K/F. Then for any $\varphi \in \mathrm{Gal}(K/F)$, we have

$$\varphi \,\mathrm{Gal}(K/E)\varphi^{-1} = \mathrm{Gal}(K/\varphi(E)).$$

Proof

We have the following chain of iffs:

$$\begin{aligned}
&\forall \psi \in \mathrm{Aut}(K)\ \psi \in \mathrm{Gal}(K/E) \\
&\iff \forall \alpha \in E\ \psi(\alpha) = \alpha \\
&\iff \forall \beta \in E\ \psi\varphi^{-1}(\beta) = \varphi^{-1}(\beta) \\
&\iff \forall \beta \in E\ \varphi\psi\varphi^{-1}(\beta) = \beta \\
&\iff \varphi\psi\varphi^{-1} \in \mathrm{Gal}(K/\varphi(E)).
\end{aligned}$$

□

Definition 32 (H-invariant)

*Let $K/E/F$ be a tower of fields, and $H \leq \mathrm{Aut}(K)$. We say E is **invariant** under H (or **H-invariant**) if $\forall \varphi \in H$, $\varphi(E) = E$.*

Proposition 65 (Intermediate Subfields and Normal Subfields)

Let K/F be a finite Galois extension. If E is an intermediate subfield of K/F, then TFAE:

1. *E/F is Galois.*
2. *E is $\mathrm{Gal}(K/F)$-invariant.*
3. *$\mathrm{Gal}(K/E) \trianglelefteq \mathrm{Gal}(K/F)$.*

Proof

By definition and Proposition 64, we immediately have (2) $\iff$ (3).

(1) $\implies$ (2) Suppose E/F is Galois. Let $\varphi \in G := \mathrm{Gal}(K/F)$. Since E/F is Galois, in particular, normal, we know that $\varphi \restriction_E \in \mathrm{Gal}(E/F)$. Thus we have $\varphi \restriction_E (E) = \varphi(E) = E$ by the surjectivity of φ [1]. It follows that E is G-invariant, simply by definition.

[1] Note that φ is a automorphism, in particular, bijective.

(2) $\implies$ (1) Suppose E is G-invariant, where again we let $G := \mathrm{Gal}(K/F)$. Now by A7, since $K/E/F$ is a tower of fields, we have that E/F is separable. Thus it suffices for us to show that E/F is normal.

Let $\alpha \in E$ with minimal polynomial $f(x) \in F[x]$. [2] Since K/F is normal, since $\alpha \in E \subseteq K$, we have that its minimal polynomial $f(x)$ must split in K. Then let $\beta \in K$ be an F-conjugate of α. Since $f(x) \in F[x]$ is irreducible, we have that G is transitive by Corollary 50, and so $\exists \varphi \in G$ such that $\varphi(\alpha) = \beta$. Then by assumption, we have that

$$\beta = \varphi(\alpha) \in \varphi(E) = E.$$

[2] ~~I think there was a slight oversight during lectures. The original reasoning here was that since K/F is normal, we have $f(x)$ splits over K. But that is not necessarily true. Being a Galois extension only requires K to be the splitting field of some non-constant polynomial (and separability of the extension), but it does not necessitate that K is where all polynomials in $F[x]$ split. This is only true if K is the algebraic closure of $F[x]$.~~ My mistake! The reasoning is correct by the normality theorem.

It follows that E/F is indeed normal. □

A natural question to ask:

> *In what way is* $\mathrm{Gal}(E/F)$ *related to* $\mathrm{Gal}(K/F)$*?*

Proposition 66 (First Isomorphism Theorem on Galois Groups)

Suppose we have a tower of fields $K/E/F$, and K/F is a finite Galois extension. If E/F is Galois, then

$$\mathrm{Gal}(E/F) \simeq \mathrm{Gal}(K/F) \Big/ \mathrm{Gal}(K/E).$$

Proof

Consider the function $\psi : \mathrm{Gal}(K/F) \to \mathrm{Gal}(E/F)$ given by $\psi(\varphi) = \varphi \restriction_E$. Note that this is a homomorphism: for $\varphi_1, \varphi_2 \in \mathrm{Gal}(K/F)$, observe that

$$\psi(\varphi_1\varphi_2) = (\varphi_1\varphi_2) \restriction_E = \varphi_1 \restriction_{\varphi_2 \restriction_E} \varphi_2 \restriction_E = \varphi_1 \restriction_E \varphi_2 \restriction_E = \psi(\varphi_1)\psi(\varphi_2).$$

It is clear that $\ker \psi = \mathrm{Gal}(K/E)$. It follows from the **First Isomorphism Theorem** that

$$\mathrm{Gal}(E/F) \simeq \mathrm{Gal}(K/F) \Big/ \mathrm{Gal}(K/E),$$

which is what we want. □

26.2 *Special Galois Groups*

Example 26.2.1

Compute $\mathrm{Gal}\left(\mathbb{Q}(\zeta_n) \Big/ \mathbb{Q}\right)$.

Solution

Note that $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is the splitting field for the separable polynomial $\Phi_n(x)$ over $\mathbb{Q}$. Thus $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois. We also know that

$$\left|\mathrm{Gal}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right)\right| = \varphi(n),$$

where we note that $\varphi(n)$ here is the **Euler φ-function**, for the sake of clarity.

Claim: $G = \mathrm{Gal}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right) \simeq \mathbb{Z}_n^\times$ Consider the map

$$\psi : \mathbb{Z}_n^\times \to G \text{ given by } \psi(k) = \varphi_k,$$

where $\varphi_k(\zeta_n) = \zeta_n^k$.

ψ is a homomorphism Observe that

$$\varphi_k \circ \varphi_l(\zeta_n) = \varphi_k(\zeta_n^l) = \zeta_n^{kl} = \varphi_{kl}(\zeta_n).$$

Thus we have $\psi(k)\psi(l) = \psi(kl)$.

ψ is injective Observe that

$$k \in \ker\psi \iff \psi(k) = 1 \iff \zeta_n^k = \zeta_n \iff k = 1.$$

ψ is surjective Notice that $|\mathbb{Z}_n^\times| = \varphi(n) = |G|$, where φ is the Euler φ-function. It follows from the injectivity of ψ that ψ is surjective.

Therefore, ψ is an isomorphism, which is what is required.

Example 26.2.2

Compute $G = \mathrm{Gal}\left(\mathbb{F}_{p^n}/\mathbb{F}_p\right)$.

Solution

First, note that $\mathbb{F}_{p^n}$ is the splitting field of the separable polynomial $x^{p^n} - x$ over $\mathbb{F}_p$. So $\mathbb{F}_{p^n}/\mathbb{F}_p$ is indeed Galois and we are not making a fool out of ourselves.

Consequently, we have that

$$\left|\mathrm{Gal}\left(\mathbb{F}_{p^n}/\mathbb{F}_p\right)\right| = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n.$$

Consider the **Forbenius map**

$$\varphi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n} \text{ given by } \varphi(a) = a^p.$$

By **Fermat's Little Theorem**, $a^p = a$, and so we have that $\varphi \in G$.

Let $j = |\varphi|$. Note that $j \leq n$ [3]. Now by definition, every element of $\mathbb{F}_{p^n}$ is a root of $x^{p^j} - x$, i.e. $p^j \geq p^n$, which implies $j \geq n$.

[3] **Why?**

Thus $|\varphi| = j = n$. It follows that

$$\text{Gal}\left(\mathbb{F}_{p^n} \Big/ \mathbb{F}_p\right) = \langle \varphi \rangle \simeq \mathbb{Z}_n.$$

27 Lecture 27th Mar 18th

27.1 Galois Groups of Polynomials

We know how hard it is to find roots of a polynomial. It would be ideal if we can find ways to work around them when trying to construct Galois groups.

Definition 33 (Discriminant)

Let $f(x) \in F[x]$ be non-constant, with K being its splitting field. We can write

$$f(x) = u(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n) \in K[x].$$

*We define the **discriminant** of $f(x)$ as*

$$\operatorname{disc} f(x) := \prod_{i<j}(\alpha_i - \alpha_j)^2.$$

Remark 27.1.1

1. *Note that*

$$\operatorname{disc} f(x) \neq 0 \iff f(x) \text{ is separable}$$

2. *For a **quadratic***

$$f(x) = x^2 + bx + c = (x-\alpha)(x-\beta) = x^2 - (\alpha+\beta) + \alpha\beta,$$

we have that its discriminant is

$$\begin{aligned}\operatorname{disc} f(x) &= (\beta-\alpha)^2 = \alpha^2+\beta^2-2\alpha\beta \\ &= (\alpha+\beta)^2 - 4\alpha\beta \\ &= (-b)^2 - 4c.\end{aligned}$$

One may note that the discriminant is like a generalization from this.

Lemma 67 (The Discriminant Lives in the Base Field)

Let $f(x) \in F[x]$ be non-constant. Then $\operatorname{disc} f(x) \in F$.

Proof

We break this into two cases:

$f(x)$ is not separable In this case $\operatorname{disc} f(x) = 0 \in F$.

$f(x)$ is separable Notice that for any $\varphi \in G = \operatorname{Gal} f(x)$, we have

$$\varphi(\operatorname{disc} f(x)) = \operatorname{disc} f(x),$$

since φ is an automorphism, in particular, a homomorphism. Thus we have that $\operatorname{disc} f(x) \in \operatorname{Fix} G = F$. □

Proposition 68 (Galois Group of Finite Extensions)

Suppose $\operatorname{Char} F \neq 2$, *$f(x)$ a separable polynomial with* $\deg f = n \geq 2$, *and $G = \operatorname{Gal} f(x)$. Let*

$$d = \prod_{i<j}(\alpha_i - \alpha_j),$$

where the α_i's are the roots of $f(x)$ in its splitting field K. If $\gamma \in G \subseteq S_n$, then $\varphi(d) = \pm d$. Moreover, $\varphi(d) = d \iff \varphi \in A_n$, and $\operatorname{Gal}\left(K \Big/ F(d)\right) = G \cap A_n$.

Also, $G \subseteq A_n \iff d \in \operatorname{Fix}(F) = F \iff \operatorname{disc} f(x)$ is a square in F.

Proof

Let $\varphi \in G$. Since we have $\operatorname{Char} F \neq 2$, we have that d and $\varphi(d)$ are roots of

$$x^2 - d^2 = x^2 - \operatorname{disc} f(x) \in F[x].$$

It follows that $\varphi(d) = \pm d$, as we want.

Observe that S_n acts on $X = \{d, -d\}$ by

$$\sigma \cdot \prod(\alpha_i - \alpha_j) = \prod(\alpha_{\sigma(i)} - \alpha_{\sigma(j)}).$$

Moreover, observe that

$$\varepsilon \cdot d = d \text{ and } (n\ (n-1)) \cdot d = -d.$$

It follows that the group action is transitive. By the Orbit-Stabilizer Theorem, we have that

$$n! = |S_n| = |\operatorname{stab}(d)|\,|\operatorname{orb}(d)| = 2\,|\operatorname{stab}(d)|\,.$$

Thus $|\operatorname{stab}(d)| = \frac{n!}{2}$, and since $\operatorname{stab}(d) \leq S_n$, it follows that $\operatorname{stab}(d) = A_n$. This also means that

$$\varphi(d) = d \iff \varphi \in A_n = \operatorname{stab}(d).$$

The rest of the statement follows immediately by the way they are introduced. □

27.1.1 *Quadratics*

Note that $\operatorname{disc} f(x)$ is not a square in F

$\iff \operatorname{Gal} f(x) \not\subseteq A_2 = \{1\}$

$\iff \operatorname{Gal} f(x) = S_2 \simeq \mathbb{Z}_2$

$\iff f(x)$ is irreducible.

We mostly know how to deal with quadratics, especially since we have a formula for finding roots of quadratic polynomials, in particular the

quadratic formula: given $f(x) = ax^2 + bx + c$, we have

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

27.1.2 *Cubics*

Recall that if $f(x) \in F[x]$ is irreducible and separable, then $\operatorname{Gal} f(x) \leq S_3$ is transitive, and so either

$$\operatorname{Gal} f(x) \simeq S_3 \text{ or } \operatorname{Gal} f(x) \simeq A_3.$$

One may find it rather difficult to find roots for cubics, especially when the **rational roots theorem** does not give us any results.

Definition 34 (Depressed Cubic)

Suppose $\operatorname{Char} F \notin \{2, 3\}$. *Let*

$$g(x) = x^3 + \alpha x^2 + \beta x + \gamma \in F[x]$$

be irreducible and separable. Let

$$f(x) = g\left(x - \frac{\alpha}{3}\right) = x^3 + bx + c \in F[x].$$

$f(x)$ *is called a* ***depressed cubic****.*

Note 27.1.1

We can derive a formula for b and c in the depressed cubic, in particular they are

$$b = \beta - \frac{1}{3}\alpha^2 \text{ and } c = \gamma + \frac{2}{27}\alpha^3 - \frac{1}{3}\alpha\beta.$$

It is important to note that $f(x)$ *is still irreducible and separable, and most importantly*

$$\operatorname{Gal} f(x) = \operatorname{Gal} g(x).$$

This is exactly why we want to consider depressed cubics, since they are easier to deal with, especially when we need to do ***long division****.*

Furthermore, if we let $\alpha_1, \alpha_2, \alpha_3$ be the roots of $f(x)$, then one can derive that

$$\operatorname{disc} f(x) = -4b^3 - 27c^2.$$

Then by 💧 *Proposition 68, we have that*

$$\operatorname{Gal} f(x) = \begin{cases} A_3 & \operatorname{disc} f(x) = d^2,\ d \in F \\ S_3 & \textit{otherwise} \end{cases}$$

Example 27.1.1

Consider the polynomial $f(x) = x^3 - 3x + 1 \in \mathbb{Q}[x]$. If we use the Mod-2 irreducibility test, one can immedaitely see that it is an irreducible polynomial that we have seen before. Thus $f(x)$ itself is irreducible.

We have that

$$\operatorname{disc} f(x) = -4(-3)^3 - 27(1)^2 = 3 \cdot 27 = 9^2,$$

and $9 \in \mathbb{Q}$. It follows that $\operatorname{Gal} f(x) \simeq A_3$. 🔨

28 Lecture 28 Mar 20th

28.1 Galois Groups of Polynomials (Continued)

28.1.1 Quartics

Definition 35 (Depressed Quartic)

Suppose $\operatorname{Char} F \neq 2$. *Given*

$$f(x) = x^4 + \alpha x^3 + \beta x^2 + \gamma x + \delta \in F[x],$$

we shall consider

$$g(x) = f\left(x - \frac{\alpha}{4}\right) = x^4 + bx^2 + cx + d \in F[x].$$

This is similarly called a ***depressed quartic****.*

Note 28.1.1

Furthermore, $\operatorname{Gal}(f(x)) = \operatorname{Gal}(g(x))$.

$g(x)$ is irreducible and separable iff $f(x)$ is irreducible and separable.

Let

$$f(x) = x^4 + bx^2 + cx + d \in F[x],$$

If $G = \operatorname{Gal}(f(x))$, then G is a transitive of S_4, with $4 \mid |G|$.

Thus our options are:

$$S_4, A_4, D_4, V, \mathbb{Z}_4,$$

where V is the Klein-4 group [1],

$$V = \{\varepsilon, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2.$$

[1] This is very **important**.

Suppose the roots of $f(x)$ are $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ which are distinct, and let $K = F(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$. Also, let

$$\begin{aligned} u &= \alpha_1\alpha_2 + \alpha_3\alpha_4 \\ v &= \alpha_1\alpha_3 + \alpha_2\alpha_4 \\ w &= \alpha_1\alpha_4 + \alpha_2\alpha_3. \end{aligned}$$

Definition 36 (Resolvent Cubic)

The resolvent cubic of $f(x)$ is defined by

$$\begin{aligned} \operatorname{Res} f(x) &= (x-u)(x-v)(x-w) \\ &= x^3 - bx^2 - 4dx + 4bd - c^2 \in F[x]. \end{aligned}$$

Let $L = F(u, v, w)$. Then $K/L/F$ is a tower of fields [2]. Now let $G = \operatorname{Gal}(f(x))$. Note that K/F is Galois. Thus K/L is Galois [3].

[2] K is the splitting field of $f(x)$ and L is the splitting field of $\operatorname{Res} f(x)$.
[3] By A7.

Also

$$\operatorname{Gal}(\operatorname{Res} f(x)) = \operatorname{Gal}(L/F),$$

where L/F is also Galois.

Since $\operatorname{Gal}(K/L) = G \cap V$ and L/F is Galois, we have that

$$\operatorname{Gal}(K/L) \trianglelefteq \operatorname{Gal}(K/F),$$

and

$$\operatorname{Gal}(\operatorname{Res} f(x)) = \operatorname{Gal}(L/F) = G/(G \cap V).$$

Let $m = |\mathrm{Gal}(\mathrm{Res}\, f(x))| = |\mathrm{Gal}(L/F)|$. Then we have the following possibilities: Note that the $m = 2$ can be a problem.

G	S_4	A_4	D_4	V	$\mathbb{Z}_4$
$G \cap V$	V	V	V	V	$\mathbb{Z}_2$
$G/G \cap V$	S_3	$\mathbb{Z}_3$	$\mathbb{Z}_2$	$\{1\}$	$\mathbb{Z}_2$
m	6	3	2	1	2

Table 28.1: Galois group G

Remark 28.1.1

G is uniquely determined when $m \in \{1, 3, 6\}$.

For the rest of our discussion, we shall focus on when $m = 2$.

We know that $G \simeq D_4$ or $G \simeq \mathbb{Z}_4$. Fortunately, the two groups have different order.

Since $\deg \mathrm{Res}\, f(x) = 3$, and $m = 2$, thus $f(x)$ factors into a linear and quadratic terms. Thus exactly one of either u, v, or w is in F. Wlog, $u \in F$.

Either option for G has a 4-cycle which fixes u. Therefore

$$\sigma = (1\,3\,2\,4) \in G.$$

Note that $\sigma^2 = (1\,2)(3\,4) \in G$.

Consider:

$$(x - \alpha_1\alpha_2)(x - \alpha_3\alpha_4) = x^2 - ux + d$$

and

$$(x - (\alpha_1 + \alpha_2))(x - (\alpha_3 + \alpha_4)) = x^2 + (b - u).$$

Claim $G = \langle\sigma\rangle \simeq \mathbb{Z}_4$ iff both of these polynomials split over L.

Proof

$(\implies)$ Suppose $G = \langle\sigma\rangle$. Then

$$\mathrm{Gal}(K/L) = G \cap V = \langle\sigma^2\rangle.$$

Thus $\alpha_1\alpha_2$, $\alpha_3\alpha_4$, $\alpha_1 + \alpha_2$, $\alpha_3 + \alpha_4 \in \mathrm{Fix}\langle\sigma^2\rangle = L$.

($\Longleftarrow$) Suppose $\alpha_1\alpha_2, \alpha_3\alpha_4, \alpha_1+\alpha_2, \alpha_3+\alpha_4 \in L$. We need only to show that $\langle\sigma\rangle$ has at most order 4.

Note that $\alpha_1\alpha_2 \in L(\alpha_1) \implies \alpha_1, \alpha_2 \in L(\alpha_1)$. Further, $v - w = (\alpha_1 - \alpha_2)(\alpha_3 - \alpha_4) \in L$. Thus $\alpha_3 - \alpha_4 \in L(\alpha_1)$, which means $\alpha_3 \in L(\alpha_1) \implies \alpha_4 \in L(\alpha_1)$. [4].

[4] Note that we needed Char $F \neq 2$.

Therefore $K = F(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = L(\alpha_1)$. Hence, $[K : L] = [L(\alpha_1) : L] = |\mathrm{Gal}(K/L)|$.

This means that if we consider

$$p(x) = x^2 - (\alpha_1 + \alpha_2)x + \alpha_1\alpha_2 \in L[x],$$

then $p(\alpha_1) = 0$. Therefore, $[K : L] \leq 2$. This implies that $[K : F] = [K : L][L : F] = 2[K : L] \leq 4$.

Since $G \simeq \mathbb{Z}_4$ or $G \simeq D_4$ with $|G| \leq 4$, we have that

$$G = \langle\sigma\rangle \simeq \mathbb{Z}_4.$$

□

❝ Note 28.1.2

Rework this entire lecture to work out the reasoning.

Part IV

Solvability by Radicals

29 Lecture 29 Mar 22nd [dirty]

29.1 Galois Groups of Polynomials (Continued 2)

29.1.1 Quartics (Continued)

Example 29.1.1

Let $f(x) = x^4 - 2x - 2 \in \mathbb{Q}[x]$. This is irreducible by 2-Eisenstein and $\mathbb{Q}$ is perfect. The resolvent of $f(x)$ is

$$\operatorname{Res} f(x) = x^3 + 8x - 4.$$

This guy has no rational roots [1], and so $\operatorname{Res} f(x)$ is irreducible.

[1] Check!

Now

$$\operatorname{disc} \operatorname{Res} f(x) = -4(8^3) - 27((-4)^2) < 0,$$

thus $\operatorname{disc} \operatorname{Res} f(x)$ is not a square in $\mathbb{Q}$. THus

$$\operatorname{Gal} \operatorname{Res} f(x) = S_3.$$

It follows that

$$\operatorname{Gal} f(x) = S_4.$$

Example 29.1.2

Let $g(x) = x^4 + 5x + 5 \in \mathbb{Q}[x]$. $g(x)$ is irreducible 5-Eisenstein and separable. We have

$$\operatorname{Res} g(x) = x^3 - 20x - 25.$$

Note that $\operatorname{Res} g(5) = 0$, and so

$$\operatorname{Res} g(x) = (x-5)(x^2+5x+5),$$

and the second guy is irreducible, again, by 5-Eisenstein. Thus

$$\operatorname{Gal} \operatorname{Res} g(x) = \mathbb{Z}_2.$$

Thus $m = 2$. Let $u = 5 \in \mathbb{Q}$, and consider

$$x^2 - 5x + 5 \text{ and } x^2 - 5.$$

Notice that the roots of $x^2 + 5x + 5$ are

$$\frac{-5 \pm \sqrt{25-20}}{2} = \frac{-5 \pm \sqrt{5}}{2}.$$

Thus $L = \mathbb{Q}(\sqrt{5})$. The roots of $x^2 - 5x + 5$ are

$$\frac{5 \pm \sqrt{5}}{2} \in L,$$

and the roots of $x^2 - 5$ are:

$$\pm\sqrt{5} \in L.$$

Thus both the polynomial splits in L and so

$$\operatorname{Gal} f(x) = \mathbb{Z}_4.$$

29.2 Solvability by Radicals

29.2.1 Solvable Groups

Definition 37 (Solvable Groups)

*A group G is **solvable** if there exists a finite chain of subgroups starting at $G = G_0$:*

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_n = \{1\},$$

where each $G_{i+1} \trianglelefteq G_i$, and G_i / G_{i+1} is abelian.

Note 29.2.1

It is not necessary that $G_{i+1} \trianglelefteq G_{i-1}$.

Example 29.2.1

Abelian $\implies$ solvable $\because G \supseteq \{1\}$.

Example 29.2.2

S_4 is solvable:

$$S_4 \supseteq A_4 \supseteq V \supseteq \{1\}.$$

Example 29.2.3

D_{2n} is always solvable since it always have a $\mathbb{Z}_n$ as a normal subgroup.

Example 29.2.4

Suppose G is simple (no non-trivial normal subgroup). Then G is solvable iff G is abelian.

Example 29.2.5

Since A_5 is simple (by Sylow) and non-abelian, we have that A_5 is **not solvable**.

Proposition 69 (Subgroups of Solvable Groups are Solvable)

Let G be a solvable groups. If $N \leq G$, then N is solvable. If $N \trianglelefteq G$, then G/N is solvable.

Proof (sketch)

We know

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_n = \{1\}.$$

Then

$$N = N \cap G_0 \supseteq N \cap G_1 \supseteq \ldots \supseteq N \cap G_n = \{1\}.$$

We know that $N \cap G_{i+1} \trianglelefteq N \cap G_i$. Also, by the **Second Isomorphism Theorem** [2],

[2] $AB/B \simeq A/A \cap B$

$$N \cap G_i / N \cap G_{i+1} \simeq (N \cap G_i)G_{i+1}/G_{i+1} \subseteq G_i/G_{i+1},$$

where the last guy is abelian. Thus N is solvable.

We have

$$G/N = \overline{G}_0 \supseteq \overline{G}_1 \supseteq \ldots \supseteq \overline{G}_n = \overline{\{1\}}.$$

Note that $\overline{G}_i/\overline{G}_{i+1} = (G_iN/N) \,/\, (G_{i+1}N/N) \simeq G_iN/G_{i+1}N$ by the **Third Isomorphism Theorem**.

Go check that the last guy is abelian. □

30 Lecture 30 Mar 25th

30.1 Solvability by Radicals (Continued)

Proposition 70 (Converse of Proposition 69)

Let $N \trianglelefteq G$. Then G is solvable iff N and G/N are solvable.

Proof

($\Longrightarrow$) This is done by Proposition 69.

($\Longleftarrow$) Given the assumptions, consider the chains

$$N = N_0 \supseteq N_1 \supseteq \ldots \supseteq N_m = \{1\} \tag{30.1}$$

and

$$\overline{G} = \overline{G}_0 \supseteq \overline{G}_1 \supseteq \ldots \supseteq \overline{G}_l = \overline{N} = \{N\},$$

where for convenience, we write

$$\overline{G}_i = G_i/N, \text{ for } G_i \leq G,\ N \subseteq G_i.$$

By the Third Isomorphism Theorem, we have that

$$\overline{G}_i \Big/ \overline{G}_{i+1} \simeq G_i \Big/ G_{i+1},$$

and in particular

$$G_{i+1} \trianglelefteq G_i.$$

Thus, we have that

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq N$$

and then by Equation (30.1), we can continue the chain down to the trivial subgroup, i.e.

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq N \supseteq N_1 \supseteq \ldots \supseteq \{1\}. \qquad \square$$

Note 30.1.1

*Suppose G is a finite solvable group. By **refining** [1] the chain as much as possible, wma*

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_n = \{1\},$$

such that $G_i \big/ G_{i+1}$ is abelian and $G_{i+1} \trianglelefteq G_i$. The refinement process means that $\nexists H_i \leq G$ such that

$$G_{i+1} \subsetneq H_i \subsetneq G_i \text{ and } G_{i+1} \trianglelefteq H_i \trianglelefteq G_i.$$

Note that if such H's exists, then we would automatically have

$$G_i \big/ H_i \text{ and } H_i \big/ G_{i+1} \text{ both being abelian,}$$

but this would mean that the refinement process was not sufficient in the first place.

Following that, we know that after refinement, it is necessary that each $G_i \big/ G_{i+1}$ is abelian and simple. This means that each $G_i \big/ G_{i+1}$ has prime order [2]

[1] By refining, we mean to make the chain of normal subgroups as long as possible.

[2] **Why?**

Definition 38 (Simple Radical Extension)

*We say that K/F is a **simple radical extension** if $K = F(\alpha)$ for some $\alpha \in K$ such that $\alpha^n \in F$ for some $n \in \mathbb{N}$.*

Definition 39 (Radical Tower)

A radical tower of F is a tower of fields

$$K_m / K_{m-1} / \dots / K_2 / K_1 / F \tag{30.2}$$

such that K_1/F and each K_{i+1}/K_i is a simple radical extension.

Definition 40 (Radical Extension)

We say that K/F is a radical extension (or just radical) if there exists a radical tower over F starting at K, i.e.

$$K_m = K$$

in Equation (30.2).

Definition 41 (Solvable by Radicals)

We say that $f(x) \in F[x]$ is solvable by radicals over F if its splitting field is contained in a radical extension of F.

Example 30.1.1

Consider $f(x) = x^3 - 5 \in \mathbb{Q}[x]$. Then we have

$$\mathbb{Q}(\sqrt[3]{5}, \zeta_3) \supseteq \mathbb{Q}(\sqrt[3]{5}) \supseteq \mathbb{Q}.$$

Note that $\zeta_3^3 = 1$ and $\left(\sqrt[3]{5}\right)^3 = 5$, both of which are in $\mathbb{Q}$. It follows that $\mathbb{Q}(\sqrt[3]{5}, \zeta_3)$ is radical and so $f(x)$ is solvable by radicals.

Example 30.1.2

Consider $f(x) = x^4 - 4x^2 + 2 \in \mathbb{Q}[x]$. Then we have

$$\mathbb{Q}(\sqrt{2+\sqrt{2}}) \supseteq \mathbb{Q}(\sqrt{2}) \supseteq \mathbb{Q}.$$

Once again, we see that $f(x)$ is solvable by radicals.

An uninteresting non-example would be $K = F(\pi)$, which is not a radical extension, and particularly because π is transcendental over Q.

We shall see a more interesting example in A10Q2.

Definition 42 (Cyclic Extension)

*We say that K/F is a **cyclic extension** if K/F is finite and Galois, and its Galois group is cyclic.*[3]

[3] In other words, we say that a finite Galois extension is cyclic if its Galois group is cyclic.

Note 30.1.2

For the rest of the course, we shall always assume that we are working in a field of characteristic 0.

Proposition 71 (Simple Primitive Extensions are Cyclic)

If F contains a primitive n^{th} root of unity and $K = F(\alpha)$ with $\alpha^n \in F$, then K/F is cyclic.

Proof

Strategy
We can show that the Galois group G to be isomorphic to a cyclic group, and we know that we can show that by showing how G permutes its roots. Since our extension contains a primitive n^{th} of unity, if we make use of that, we will have a way of moving around all n of the roots. The polynomial which captures all of the roots we want is exactly $f(x) = x^n - \alpha^n$.

Consider the polynomial

$$f(x) = x^n - \alpha^n \in F[x].$$

Let $\zeta \in F$ we a primitive n^{th} root of unity. Now the roots of $f(x)$ in K are

$$\alpha, \alpha\zeta, \alpha\zeta^2, \ldots, \alpha\zeta^{n-1}.$$

We see that K is the splitting field of $f(x)$ over F. Since F is perfect (this is our assumption for the rest of the course!), we know that K/F is therefore Galois.

Now for each $\varphi \in G = \text{Gal}(K/F)$, $\exists!0 \leq i \leq n-1$ such that $\varphi(\alpha) = \alpha\zeta^i$. Let $\Gamma : G \to \mathbb{Z}_n$ such that $\Gamma(\varphi) = i$.

It is clear that Γ is a homomorphism: taking two elements is the same as just adding the powers. It is also injective, which is rather clear, since each of the $\varphi \in G$ has a uniquely associated $0 \leq i \leq n-1$.

It follows that $G \simeq \mathbb{Z}_n$ by the First Isomorphism Theorem, and so G is cyclic. □

31 Lecture 31 Mar 27th

31.1 Solvability by Radicals (Continued 2)

Definition 43 (Linearly Dependent and Independent)

We say that $\{\sigma_1, \sigma_2, \ldots, \sigma_n\} \subseteq \operatorname{Aut} K$ *is* ***linearly dependent*** *over* K *if* $\exists a_i \in K$, *with not all* $a_i \neq 0$ *such that*

$$a_1\sigma_1(\alpha) + \ldots a_n\sigma_n(\alpha) = 0$$

for all $\alpha \in K$.

Otherwise, we say that $\{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ *is* ***linearly independent****.*

Lemma 72 (The Galois Group is Linearly Independent)

Suppose $[K : F] < \infty$, *Then* $\operatorname{Gal}(K/F)$ *is linearly independent over* K.

Proof

Suppose not. Let $\{\sigma 1, \ldots, \sigma_r\}$ be a minimal linearly dependent subset of $G = \operatorname{Gal}(K/F)$. Notice that since $a_1 \in K^\times$ m we have that $a_1\sigma_1(\alpha) = 0$ for any $\alpha \in K$ implies that $\sigma_1 = 0$, which is impossible. Thus we must have $r > 1$.

Now by assumption, $\exists \alpha_i \in K$ such that $\forall \alpha \in K$, we have

$$a_1\sigma_1(\alpha) + a_2\sigma_2(\alpha) + \ldots + a_r\sigma_r(\alpha) = 0.$$

Let $\beta \in K$ such that wlog, $\sigma_1(\beta) \neq \sigma_2(\beta)$. Then for any $\alpha \in K$, we have

$$a_1\sigma_1(\alpha)\sigma_1(\beta) + a_2\sigma_2(\alpha)\sigma_2(\beta) + \ldots + a_r\sigma_r(\alpha)\sigma_r(\beta) = 0 \tag{31.1}$$

and

$$a_1\sigma_1(\alpha)\sigma_1(\beta) + a_2\sigma_2(\alpha)\sigma_1 + \ldots + a_r\sigma_r(\alpha)\sigma_1(\beta) = 0. \tag{31.2}$$

Subtracting Equation (31.2) from Equation (31.1), we have

$$[a_2\sigma_2(\beta) - a_2\sigma_1(\beta)]\sigma_2(\alpha) + \ldots + [a_r\sigma_r(\beta) - a_r\sigma_1(\beta)]\sigma_r(\alpha) = 0.$$

Notice that the cofficient of first term is non-zero. Thus $\{\sigma_2, \ldots, \sigma_r\}$ is also a linearly dependent subset of G. This contradicts minimality, and so it is impossible that G is linearly dependent. □

Proposition 73 (Cyclic Extensions over Base with Primitive Roots are Simple Radical)

Let F be a field, which contains a primitive n^{th} root of unity ζ. If K/F is cyclic with $[K : F] = n$, then K/F is simple radical.

Proof

[1]By assumption, we may assume that

$$G = \mathrm{Gal}(K/F) = \langle\sigma\rangle, \text{ where } |\sigma| = n = [K : F] = |G|,$$

for some $\sigma \in G$.

Finding an element that will serve as the adjoined element

For any $\alpha \in K$, consider

$$g(\alpha) = \alpha + \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) + \ldots + \zeta^n\sigma^n(\alpha).$$

Notice that since ζ is a primitive n^{th} of unity, we have that

$$\zeta\sigma(g(\alpha)) = g(\alpha) \implies \sigma(g(\alpha)) = \zeta^{-1}g(\alpha) = \zeta^{n-1}g(\alpha).$$

[1] This is a proof that involves a lot of non-trivial steps. Each of these steps are given a mark.

Since σ is automorphism, in particular a homomorphism, we have that

$$\sigma(g(\alpha)^n) = \sigma(g(\alpha))^n = (\zeta^{n-1} g_(\alpha))^n = g(\alpha).$$

It follows that $g(\alpha) \in \operatorname{Fix} G = F$. Note that since $\alpha \in K$ was arbitrary, this process works for any α.

Showing that $g(\alpha)$ cannot live in any of the intermediate extensions

Now since G is linearly independent over K (by Lemma 72), we know that $\exists \alpha \in K$ such that $g(\alpha) \neq 0$. Let's consider such an α. By our argument just slightly before this, we know that

$$\sigma^i(g(\alpha)) \neq g(\alpha) \text{ for } 1 \leq i \leq n-1.$$

This means that $g(\alpha) \notin \operatorname{Fix} H$ for any $\{1\} \neq H \leq G$. It follows from the Fundamental Theorem of Galois Theory that $g(\alpha) \notin E$ for any $F \subseteq E \subsetneq K$. It thus follows that $F(g(\alpha)) = K$.

Since $g(\alpha)^n \in F$, it follows by definition that K/F is a simple radical. □

The following proposition is important for us to move forward, but we shall prove this in Chapter 32.

Proposition (A Condition for Solvable Galois Groups)

Suppose we have a tower of fields $K/E/F$, K/E is radical, and E/F is Galois. Then there exists L/K such that

- *L/F is Galois;*
- *L/E is radical; and*
- *$\operatorname{Gal}(L/E)$ is solvable.*

Corollary 74 (Radical Extensions have Solvable Extensions)

If K/F is radical, then there exists L/K such that L/F is radical and Galois, with $\operatorname{Gal}(L/F)$ being solvable.

Proof

We simply need to use the last proposition and set $E = F$. □

Theorem 75 (Galois Theorem)

Let $f(x) \in F[x]$. Then $f(x)$ is solvable by radicals over F iff $\mathrm{Gal}(f(x))$ is solvable.

Proof

[2] Suppose $f(x)$ is solvable by radicals over F. WMA

$$f(x) = p_1(x)^{i_1} p_2(x)^{i_2} \dots p_l(x)^{i_l},$$

where each $p_i(x)$ is irreducible and distinct from one another. Now by replacing $f(x)$ with $p_1(x)p_2(x)\dots p_l(x)$, [3] wma $f(x)$ is separable.

Let E be the splitting field $f(x)$ over F. Then E/F is Galois [4]. Moreover, since $f(x)$ is, still, solvable by radicals, we have that $E \subseteq K$ where K/F is a radical extension. By Corollary 74, $\exists L/K$ such that L/F is Galois and radical, and in particular $\mathrm{Gal}(L/F)$ is solvable.

Since E/F is Galois, we have that $\mathrm{Gal}(L/E) \trianglelefteq \mathrm{Gal}(L/F)$ by Proposition 65, and by Proposition 66, we have

$$\mathrm{Gal}(f(x)) = \mathrm{Gal}(E/F) \simeq {}^{\mathrm{Gal}(L/F)}\Big/_{\mathrm{Gal}(L/E)}.$$

Since ${}^{\mathrm{Gal}(L/F)}\Big/_{\mathrm{Gal}(L/E)}$ is abelian, it follows that $\mathrm{Gal}(f(x))$ is indeed solvable. □

[2] We shall proof only the ($\Longrightarrow$) direction, which is what we will be using for the rest of the course. Please read ($\Longleftarrow$) direction in the recommended text of the course (shall be added to an appendix page if I come to read it).

[3] We may do this because $\mathrm{Gal}(f(x)) = \mathrm{Gal}(p_1(x)p_2(x)\dots p_l(x))$.

[4] cf. the fundmental theorem.

Note 31.1.1

The contrapositive of Theorem 75 is particularly useful; the statement is

> *If* $\mathrm{Gal}(f(x))$ *is not solvable, then* $f(x)$ *is not solvable by radicals.*

Warning

Going back to Chapter 30, recall the definition of solvability by radicals, and notice that Galois' Theorem does not tell us that the splitting field of $f(x)$ *need to be a radical extension, despite the splitting field being contained in a radical extension.*

32 Lecture 32 Mar 29th

32.1 Solvability by Radicals (Continued 3)

Recall that $f(x) \in F[x]$ is solvable by radicals iff $\operatorname{Gal} f(x)$ is solvable (cf. Galois' Theorem). Note that we still assume that $\operatorname{Char} F = 0$.

Example 32.1.1

Let $f(x) \in \mathbb{Q}[x]$ such that $1 \leq \deg f(x) < 5$. Then $f(x)$ is solvable by radicals.

Proof

We can get $f(x) \mapsto g(x)$ by deleting repeated factors. Then $g(x)$ is separable. Then $\operatorname{Gal} f(x) = \operatorname{Gal} g(x) \leq S_4$. Recall that S_4 is solvable. □

We require the following proposition from group theory. You can prove this for yourself.

Note 32.1.1

$S_n =< (1\ 2), (1\ 2\ 3\ \ldots\ n) >$. *If p is prime, then $S_p =< \tau, \sigma >$, where τ is any transposition and σ is any p-cycle.*

Lemma 76 (Galois groups of Polynomials with Non-Real Roots)

Let $f(x) \in \mathbb{Q}[x]$ be irreducible with prime degree p. If $f(x)$ has exactly 2

non-real roots, then $\operatorname{Gal} f(x) \simeq S_p$.

Proof

Let α be a root of $f(x)$ in its splitting field K. Then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg f = p$. By the Tower Theorem, $p \mid [K : \mathbb{Q}] = |\operatorname{Gal} f(x)|$. This means that $\exists \sigma \in \operatorname{Gal} f(x)$, $|\sigma| = p$. Wlog, wma $\sigma = (1\ 2\ 3\ \dots\ p)$.

Let $\varphi : \mathbb{C} \to \mathbb{C}$ be given by $\varphi(z) = \bar{z}$, which is a $\mathbb{Q}$-map [1]. By the Normality Theorem, $\varphi \restriction_K \in \operatorname{Gal} f(x)$. Since $f(x)$ has only two non-real roots, it follows that $\varphi \restriction_K = (i\ j)$.

By the note above, we have that $\operatorname{Gal} f(x) \simeq S_p$. □

[1] Indeed, φ fixes $\mathbb{Q}$

Example 32.1.2

Consider $f(x) = x^5 + 2x^3 - 24x - 2 \in \mathbb{Q}[x]$. Note that $f(x)$ is irreducible by 2-Eisenstein. Also,

$f(-100)$	$f(-1)$	$f(1)$	$f(100)$
< 0	> 0	< 0	> 0

Table 32.1: Some values of $f(x)$

We see that there are at least 3 real roots between all of the above values by the **Intermediate Value Theorem**.

Say the roots of $f(x)$ are α_i, $1 \le i \le 5$. Then, $\sum \alpha_i = -[x^4]f(x) = 0$, where $[x^4]f(x)$ is the coefficient of x^4 in $f(x)$, and

$$\sum_{i<j} \alpha_i \alpha_j = [x^3]f(x) = 2.$$

Therefore, $\sum \alpha_i^2 = (\sum \alpha_i)^2 - 2\sum_{i<j} \alpha_i \alpha_j = -4$. Thus, not all roots of $f(x)$ are real. Since non-real roots of $f(x)$ appear in conjugate pairs, it follows that $f(x)$ has exactly two non-real roots. By the lemma, $\operatorname{Gal} f(x) \simeq S_5$. Since S_5 is not solvable (cause $A_5 \le S_5$), $f(x)$ is not solvable by radicals.

(Showing Insolvability of a Quintic)

There are several ways we can do this. Again, one can mix and match these methods to show that a quintic is not solvable by radicals.

- *The above example gives us a heuristical method to check if any of the roots are non-real, and the key to the above method is to pay attention to*

$$\sum \alpha_i = -[x^4]f(x) \text{ and } \sum_{i<j} \alpha_i\alpha_j = [x^3]f(x),$$

and there will be non-real roots if

$$\sum \alpha_i^2 = \left(\sum \alpha_i\right)^2 - 2\sum_{i<j} \alpha_i\alpha_j < 0,$$

since that is not a value that we can expect coming from the reals.

- *We can also check the* ***derivative*** *of $f(x)$, and inspect from there where the 'turning points' of $f(x)$ on $\mathbb{R}^2$ are and how many are there.*

Theorem 77 (Insolvability of the Quintics)

Not every quintic $f(x) \in \mathbb{Q}[x]$ is solvable by radicals.

Example 32.1.3

An example of a quintic that is solvable by radicals is $x^5 - 1$.

Going back to that black box that we have yet to prove: recall the proposition.

Proposition 78

Suppose $K/E/F$ is a tower of fields, E/F is Galois and K/E is radical. Then $\exists L/K$ such that L/F is Galois and L/E is radical, and $\mathrm{Gal}(L/E)$ is solvable.

Proof

We prove the result when K/E is simple radical. The more general case follows by 'an' [2] induction.

Say $K = E(\alpha)$ where $\alpha^n = \beta \in E$. Also, suppose $G = \mathrm{Gal}(E/F) =$

[2] There is some work to do, but this is not important. Still a nice exercise I reckon.

$\{\sigma_1, \sigma_2, ..., \sigma_r\}$. Consider [3]

$$f(x) = \Phi_n(x) \prod_{i=1}^{r} (x^n - \sigma_i(\beta)) \in \operatorname{Fix} G[x] = F[x].$$

Let L be the splitting field for $f(x)$ over K.

L/F is Galois Notice that

$$K = K(\text{roots of } f(x)) = K(\alpha, \text{ others}) = E(\alpha, \text{ others}).$$

Thus L is the splitting field for $f(x)$ over E (L/E is radical). Since E/F is Galois, E is the splitting field of some separable polynomial $h(x) \in F[x]$. Thus L is the splitting field for $h(x)f(x)$ over F. Since $\operatorname{Char} F = 0$, L/F is Galois.

(Proof isn't done, will be added later after next Wed.) □

[3] We want to grab the n roots of unity. Notice that $\prod_{i=1}^{r}(x^n - \sigma_i(\beta))$ stays in Fix G if we apply any of the σ's. In particular, notice that for any σ_j, when applied to $f(x)$, we know that $\Phi_n(x)$ is definitely fixed, but the other requires some care. However, it is not difficult: notice that we end up with $(\sigma_j\sigma_i)(\beta)$, over all i, and for each i, we get another $\sigma_{i'}$ that is different from other i's. It is this subtle observation that eventually keeps the polynomial in the fix field.

33 Lecture 35 Apr 05th [very dirty]

33.1 Final Examination Information

Logistics

- (Mon) Apr 22 0900
- STC 0040 **(do double check before the exam)**
- Assigned seating (CHECK)

Office Hours

- Normal office hours are cancelled
- (Tue) Apr 16 1300 - 1500
- (Thu) Apr 18 1300 - 1500
- Appointment

Exam Info

- 8Q $\times$ 10m $\implies$ 80 marks total
- ordinary exam (no scaling) - easier than midterm
  - Read back on assignments and examples, etc.
- Materials
  1. minimal polynomials, field extensions
  2. show an ext K/F is Galois and find $\mathrm{Gal}(K/F)$
  3. Gal $f(x)$

4. 3 assignment-related questions (parts)
5. 2 proofs from lecture (2 part)
   - Second half of the course (post-midterm, after finite fields)

6.(a) New proof

(b) Assignment proof (from assignments)

7. Solvability by radicals stuff
8. Give examples or DNE (10 parts)

Important to read assignments for 1, 2, 3, 4, 6(★), 7, 8

Some practice problems

1. A Galois K/F such that $[K:F] = 36$. $\mathbb{Q}(\zeta_{37})/\mathbb{Q}$ (note 37 is prime)
2. An irreducible $f(x) \in \mathbb{Q}[x]$ such that $\deg f(x) = 7$ and $|(x)| = 20$.

   No, $7 \nmid 20$, transitive subgroup
3. A field E such that $\mathbb{F}_p \subseteq E \subseteq\subseteq \mathbb{F}_{p^{12}}$ such that $E/\mathbb{F}_p$ is NOT Galois.

   No, $\because \mathrm{Gal}(\mathbb{F}_{p^{12}}/\mathbb{F}_p) \simeq \mathbb{Z}_{12}$ is abelian. and

$$\mathrm{Gal}(\mathbb{F}_{p^{12}}/E) \trianglelefteq \mathrm{Gal}(\mathbb{F}_{p^{12}}/\mathbb{F}_p)$$

4. An irreducible quintic in $\mathbb{Q}[x]$ which is solvable by radicals. ($x^5 - 2$)
5. An infinite field of characteristic 7. ($\overline{\mathbb{F}_7}$, $\mathbb{Z}_7(x)$)
6. A Galois ext of $\mathbb{Z}_2(t^2)$.

   $\mathbb{Z}_2(t^2)$
7. A finite ext of $\mathbb{C}(t)$ which is not simple.

   perfect field, primitive element theorem gives simple extension
8. An irreducible polynomial in $\mathbb{F}_{3^{10}}[x]$ which is not separable.

   DNE $\because$ finite fields are perfect

A Asides and Prior Knowledge

A.1 Correspondence Theorem

The Correspondence Theorem is somewhat widely known as the Fourth Isomorphism Theorem, although some authors associates the name with a proposition known as Zaessenhaus Lemma.

Theorem A.1 (Correspondence Theorem)

Let G be a group, and $N \triangleleft G$ [1]. Then there exists a bijection between the set of all subgroups $A \leq G$ such that $A \supseteq N$ and the set of subgroups A/N of G/N.

[1] Recall that this symbol means that N is a normal subgroup of G.

Proof

Index