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

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

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

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

The orbits of x is a set

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

[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 $x \in X$, $\text{stab}(x)$ and $\text{orb}(x)$ are the stabilizers and orbits of x, respectively. Then

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

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

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

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

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)

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

---

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].

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.

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

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.

[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.

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 $p \nmid [G : C(a_i)]$. This implies that $p^n \mid |C(a_i)|$.*

This highlighted part requires clarification.

Since $a_i \notin Z(G)$, 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.

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

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

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 $HP \leq N$ [3]. 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. □

[3] 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

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

Proof

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

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

□

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

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

where s is not necessarily r. From here, it suffices to show that $Q = P_i$ for some $i \in \{1, 2, \ldots, s\}$. 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 $i \in \{1, 2, \ldots, s\}$, 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 normal subgroups.*

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 $n_7 \mid 8 = 2^3$. 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, by the Finite Abelian group structure, the distinct Sylow 8-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 [1]. 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. □

[1] 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*

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

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

Note that the second remark is not true if $G = D_6$. 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] Crap, I don't remember why...

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

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.

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

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

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

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

[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 $\left|\overline{G}\right| \in \{15,20,30\}$. [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,

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

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.

[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 $f9x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$. 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] 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

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

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

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

[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.

(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.

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.

7.2 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 following: 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 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

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

i.e. $F(\alpha_1, \ldots, \alpha_n)$ 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 $\phi : F[x] \to F(\alpha)$ by $\phi(g(x)) = g(\alpha)$. Note that this is a ring homomorphism. Let

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

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**,

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

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

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

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. (Link will be provided later)

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

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.

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

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

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 $F(c_{n-1}, \ldots, c_1, c_0)$. By the Tower Theorem,

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

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

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

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

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?

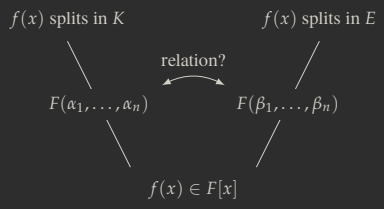

Figure 12.1: Differing Splitting Fields

Lemma 31 (Isomorphic Fields have Isomorphic Polynomial Rings)

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

Proof

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

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

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

Note 12.1.1

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

Lemma 32 (Isomorphism Extension Lemma)

Let F and F' be fields, $\phi : F[x] \to F'[x]$ 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 $\psi \restriction_F = \phi$. Moreover, $\psi(\alpha) = \beta$.

Proof (Sketch)

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

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

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

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

Let $a \in F$. Then

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

Also,

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

[1]

Exercise 12.1.1
Prove that $\phi(f(x))$ 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, $\phi : F \to F'$ an isomorphism, and K' a splitting field for $\phi(f(x))$ over F'. Then there is an isomorphism $\psi : K \to K'$ such that $\psi \restriction_F = \phi$.

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 $\phi = \mathrm{id}$ and use Lemma 33. $\square$

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

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

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

Proof

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

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

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

Following the various results that we have proven in the last few lec-

tures, 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

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

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*

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

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

Remark 13.2.2

Since $\Phi_n(x)$ has rational coefficients, and $\mathbb{C}$ is an algebraic closure of $\mathbb{Q}$, 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 $[\mathbb{Q}(\xi_n) : \mathbb{Q}] = \phi(n)$. 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

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

and the primitives are

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

Thus

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

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

Proof

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

Strategy

We shall use strong induction here.

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.

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.

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

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

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 $\mathbb{C}$).

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 $\Phi_n(x) \mid g(x)$.

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].

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

Thus, the statement which we wish to prove becomes the following: $\xi_n^{p_1}, \xi_n^{p_1 p_2}, \ldots, \xi_n^{p_1 p_2 \cdots p_N} = \alpha$ 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 $\overline{\Phi}_n(x) = \bar{g}(x)\bar{h}(x)$. It follows that $\bar{l}(x)^2 \mid \overline{\Phi}_n(x)$ [5]. Since $\overline{\Phi}_n(x) \mid x^n - 1$, we have that

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

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.

[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?**

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

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

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

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

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, $[\mathbb{Q}(\xi_n) : \mathbb{Q}] = \phi(n)$.

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

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

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 a 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 gield. 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

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

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 $\Gamma(F)$ 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 $F = \operatorname{span}_{\mathbb{Z}_p}\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$. It follows that $|F| = p^n$. □

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.

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 $\mathbb{Z}_p[x]$.

Proof

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

[3] Is it really Lagrange?

For the ■ 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 $\Gamma F = p$, 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**.

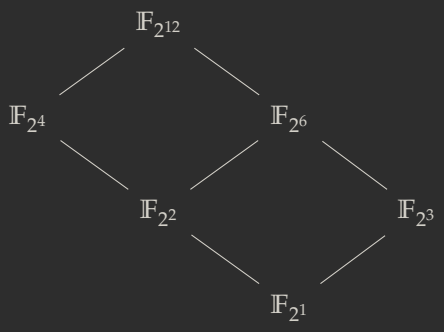

Figure 16.1: Lattice of $\mathbb{F}_{2^{12}}$

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