

**Notes on
MATH 494
(Honors Algebra II)**

April 27, 2022

Faye Jackson

CONTENTS

I. Introduction and Administration.....	2
II. Ring Theory.....	2
II.1. Group Review + Motivation.....	2
II.2. The Basics of Rings.....	4
II.3. Polynomial Rings.....	11
II.4. Ring Extensions.....	15
II.5. Basic Algebraic Geometry.....	17
II.6. Euclidean Domains, PIDs, Noetherian-ness, and UFDs.....	21
III. Midterm Review.....	31
IV. Galois Theory.....	34
IV.1. Field Extensions.....	34
IV.2. Motivation: Constructions with Straight Edge and Compass.....	36
IV.3. More Field Extensions / Splitting Fields.....	40
IV.4. Separability.....	46
IV.5. Finite Fields.....	48
IV.6. Galois Extensions, and the Fundamental Theorem.....	51
IV.7. Solvability by Radicals.....	61
V. Modules.....	64
VI. Symmetric Functions.....	69
VI.1. Basics in all Rings.....	69
Appendix A. Gauss's Lemma and its Consequences.....	73
Appendix B. The Primitive Element Theorem.....	76

I. Introduction and Administration

Two highlights of the course

- (1) We know $ax^2 + bx + c$ ($a \neq 0$) has roots

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

There is a similar formula for polynomials of degree 3 and 4, but not degree 5 or higher.

- (2) $x^2 + 2 = y^3$. The only solutions in integers are $x = \pm 5, y = 3$. Important and powerful methods lurking behind simple problems.

This course: Rings, fields, modules, Galois theory.

Administration

- HW due Mondays midnight.
- Office hours: Sunday 2pm-3:30pm
- Friday: 7-8:30pm

II. Ring Theory

II.1. Group Review + Motivation

We first recall some things

Definition II.1.1

A group $(G, *)$ is a set G with a function $*$: $G \times G \rightarrow G$ and an element $1_G \in G$ such that

- $*$ is associative
- 1_G is an identity element (therefore unique).
- For all a , there exists an a' with $aa' = 1_G = a'a$.

Consequences: 1_G is the unique identity element, inverses are unique.

We say G is abelian if $ab = ba$ for all $a, b \in G$. For abelian groups we denote the group law by addition, the identity element by 0, and inverses by negation $-a$.

Example II.1.1

\mathbb{Z} (under addition), $\mathbb{Z}/n\mathbb{Z}$ (under addition). Direct products of these.

\mathbb{R} (under addition), $\mathbb{R} \setminus \{0\}$ (under multiplication).

Definition II.1.2

A group homomorphism between groups G and H is a function $\varphi : G \rightarrow H$ such that

$$\varphi(gg') = \varphi(g)\varphi(g')$$

this implies $\varphi(1_G) = 1_H$ and $\varphi(a^{-1}) = \varphi(a)^{-1}$.

Question: What happens for abelian groups G, H . What can we say about $\text{Hom}(G, H) = \{\text{homomorphisms } G \rightarrow H\}$? Well, first this is clearly an abelian group under pointwise addition.

Example II.1.2

$\text{Hom}(\mathbb{Z}, \mathbb{Z})$, which is defined by where the generator 1 goes. Thus it is the set

$$\{[n] : i \mapsto ni \mid n \in \mathbb{Z}\} = \mathbb{Z}.$$

Then addition corresponds to addition (by distributivity), and composition corresponds to multiplication.

Likewise $\text{Hom}(\mathbb{Z} \times \mathbb{Z}, \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}) = M_{2,3}(\mathbb{Z})$ given by

$$\begin{bmatrix} * & * \\ * & * \\ * & * \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix}$$

. Again following generators (now with relations):

$$\text{Hom}(\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) = \{[n] : i \mapsto in \pmod{2} \mid n \in \mathbb{Z}/2\mathbb{Z}\}$$

$$\text{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) = \{[0]\}$$

$$\text{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}) = \{[0]\}.$$

Lemma II.1.1

If G, H are groups and H is abelian, then $\text{Hom}(G, H)$ is an abelian group under the operation which takes $\varphi, \psi \in \text{Hom}(G, H)$ and produces

$$\varphi + \psi : G \rightarrow H$$

$$g \mapsto \varphi(g) + \psi(g).$$

Proof. $\varphi + \psi \in \text{Hom}(G, H)$ because for $g, g' \in G$ we have

$$\begin{aligned} (\varphi + \psi)(g + g') &= \varphi(g + g') + \psi(g + g') \\ &= \varphi(g) + \varphi(g') + \psi(g) + \psi(g') \\ &= \varphi(g) + \psi(g) + \varphi(g') + \psi(g') \\ &= (\varphi + \psi)(g) + (\varphi + \psi)(g'). \end{aligned}$$

The identity element maps everything to 0

$$0_{\text{Hom}(G, H)} := (g \mapsto 0).$$

Inverses are given by taking $\varphi \in \text{Hom}(G, H)$ and producing

$$-\varphi : G \rightarrow H$$

$$g \mapsto -\varphi(g).$$

Then clearly $\varphi + (-\varphi) = 0 = (-\varphi) + \varphi$. Furthermore $-\varphi \in \text{Hom}(G, H)$.

The operation is clearly abelian and associative, as H satisfies both of these properties, for example

$$(\varphi + \psi)(g) = \varphi(g) + \psi(g) = \psi(g) + \varphi(g) = (\psi + \varphi)(g).$$



Refined question: For G an abelian group, what can we say about $\text{End}(G) := \text{Hom}(G, G)$? Here we have more data, namely the composition

Example II.1.3

$\text{End}(\mathbb{Z}) \cong \mathbb{Z}$ as a group under $+$, composition corresponds to \cdot .

$\text{End}(\mathbb{Z} \times \mathbb{Z}) \cong M_{2,2}(\mathbb{Z})$ under $+$, composition corresponds to \cdot .

$\text{End}(\mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$ under $+$, composition corresponds to \cdot .

Note: In each case, there is a familiar way to multiply on the right side, and it always corresponds to composition on the left side.

For $\varphi, \psi \in \text{End}(G)$, $\varphi \circ \psi : g \mapsto \varphi(\psi(g))$ is in $\text{End}(G)$.

$$\varphi(\psi(g + g')) = \varphi(\psi(g) + \psi(g')) = \varphi(\psi(g)) + \varphi(\psi(g')).$$

Properties:

- Associative
- Has an identity element $1 : g \mapsto g$.
- Distributive laws:

$$(\psi + \chi) \circ \varphi = (\psi \circ \varphi) + (\chi \circ \varphi)$$

$$\varphi \circ (\psi + \chi) = (\varphi \circ \psi) + (\varphi \circ \chi).$$

II.2. The Basics of Rings

Definition II.2.1

A ring is a set R with two functions $+, \cdot : R \times R \rightarrow R$ such that

- $(R, +)$ is an abelian group (say with identity $0 \in R$, and inverses $-r$ for every $r \in R$).
- (R, \cdot) is associative with an identity 1 .
- Distributive laws hold

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

$$(b + c) \cdot a = (b \cdot a) + (c \cdot a).$$

We thus showed that if G is an abelian group, then $\text{End}(G)$ is a ring.

Definition II.2.2

Let R, S be rings. A ring homomorphism is a function $f : R \rightarrow S$ which preserves $+, \cdot, 0, 1$, additive inverses.

In fact it suffices to preserve $+, \cdot, 1$ because the fact that f preserves $+$ implies it preserves 0 and negation.

More concretely we require

$$f(r +_R r') = f(r) +_S f(r')$$

$$f(r \cdot_R r') = f(r) \cdot_S f(r')$$

$$f(1_R) = 1_S.$$

And as a consequence $f(-r) = -f(r)$ and $f(0_R) = 0_S$.

Definition II.2.3

A subring of a ring R is a subset of R which is a ring under $+, *$ from R .

Lemma II.2.1

If R, S are rings and $f : R \rightarrow S$ is a ring homomorphism, then $f(R)$ is a subring of S (meaning it is a ring with the inherited operations).

Proof. Clearly $f(R)$ is an abelian group from last semester (as f is a homomorphism of abelian groups). We then know that $*$ is associative and distributive because these properties are inherited from S . There is also an identity element inherited from S because $f(1_R) = 1_S$.

It is then closed under multiplication because $f(rr') = f(r)f(r')$. 

Update: Added homework due dates and office hours to Section I

Recall II.2.1

The key example of a ring is $\text{End}(G)$ for G an abelian group (with $+$). Then

$$(\varphi + \psi)(g) := \varphi(g) + \psi(g)$$

$$\varphi * \psi := \varphi \circ \psi$$

In fact this situation is “universal”

Definition II.2.4


An isomorphism $f : R \rightarrow S$ is a bijective homomorphism (implying its inverse is a homomorphism as well). Rings are isomorphic if there exists an isomorphism between them.

Lemma II.2.2

For every ring R and $r \in R$, $r \cdot 0 = 0 = 0 \cdot r$.

Proof. Note that $0 + 0 = 0$, and so

$$r \cdot 0 = r(0 + 0) = r \cdot 0 + r \cdot 0$$

Cancelling $r \cdot 0$ (by additive inverses) we know that $0 = r \cdot 0$ as desired. The other direction is similar. 

Lemma II.2.3

In every ring R and for every $r \in R$, we have $(-1) \cdot r = -r = r \cdot (-1)$.

Proof. Note that $1 + (-1) = 0$. Therefore

$$(1 + (-1))r = 0 \cdot r = 0$$

$$r + (-1)r = 0.$$

Thus $(-1)r = -r$ (appealing to group theory). 

Theorem II.2.4

Every ring R is isomorphic to a subring of $\text{End}(R_+)$ (where R_+ is the additive group on R).

Concretely, there is a ring homomorphism $[-] : R \rightarrow \text{End}(R_+)$ such that the restriction $R \rightarrow \text{im}[-]$ is an isomorphism.

Proof. We then may write down the relevant homomorphism as

$$\begin{aligned} [-] : R &\rightarrow \text{End}(R_+) \\ r &\mapsto (r' \mapsto rr'). \end{aligned}$$

We know that $[r] \in \text{End}(R_+)$ by the distributive law because

$$r' + r'' \mapsto r(r' + r'') = rr' + rr'' = [r](r') + [r](r'').$$

It is then a ring homomorphism because

$$\begin{aligned} [r + s](r') &= (r + s)r' = rr' + sr' = ([r] + [s])r' \\ [rs](r') &= (rs)r' = r(sr') = [r]([s](r')) \\ [1](r) &= 1r = r \implies [1] = \text{Id}_{R_+}. \end{aligned}$$

Now because the restriction is automatically surjective we just need to show injectivity. Suppose $[r] = [s]$. Then

$$\begin{aligned} [r](1) &= r \cdot 1 = r \\ [s](1) &= s \cdot 1 = s. \end{aligned}$$

Thus $r = s$ as desired.

This completes the proof!

**Definition II.2.5** (Inverses)

Let R be a ring, and $r \in R$. We say that $s \in R$ is an inverse of r provided that

$$rs = 1 = sr.$$

If r has an inverse then we say that r is a unit in R . We write R^* or R^\times to denote the set of units in R . This is almost trivially a group under multiplication because

$$\begin{aligned} 1 \cdot 1 &= 1 \implies 1 \in R^\times \\ r_1, r_2 \in R^\times &\implies r_1 r_2 (s_2 s_1) = 1 \\ &\implies r_1 r_2 \in R^\times \end{aligned}$$

inverses are tautological.

Note: if s exists then it is unique because

$$rs = 1 = tr$$

$$s = (tr)s = t(rs) = t$$

In this case, we will denote s by r^{-1} . One can also see this from group theory, but note our proof is slightly stronger. Namely it implies

Lemma II.2.5

If r has both a left and a right inverse, then these inverses agree.

Example II.2.2

If G is an abelian group then $(\text{End}(G))^\times = \text{Aut}(G)$.

$$\text{End}(\mathbb{Z}) \cong \mathbb{Z}$$

$$\text{Aut}(\mathbb{Z}) = \{\pm 1\}$$

$$\text{End}(\mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/m\mathbb{Z}$$

$$\text{Aut}(\mathbb{Z}/m\mathbb{Z}) = \{n \in \mathbb{Z}/m\mathbb{Z} \mid \gcd(n, m) = 1\}$$

$$\text{End}(\mathbb{Z} \times \mathbb{Z}) \cong M_{2,2}(\mathbb{Z})$$

$$\text{End}(\mathbb{Z} \times \mathbb{Z}) = \{A \in M_{2,2}(\mathbb{Z}) \mid \det(A) = \pm 1\}$$

$$= \{\text{invertible } 2 \times 2 \text{ matrices over } \mathbb{Z}\}$$

Example II.2.3

Examples of rings.

$$\begin{aligned} \mathbb{Z}[\sqrt{2}] &= \left\{ \sum_{i=1}^n a_i (\sqrt{2})^i \mid a_i \in \mathbb{Z} \right\} \\ &= \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\} \end{aligned}$$

It turns out that $(\mathbb{Z}[\sqrt{2}])^\times = \{\pm(1 + \sqrt{2})^n \mid n \in \mathbb{Z}\}$.

The ring R of entire functions on \mathbb{C} (all differentiable functions on \mathbb{C} , equivalently power series with an infinite radius of convergence).

What is R^\times ? It is the set of entire functions on \mathbb{C} with no zeros. This actually turns out to be $\{e^{f(x)} \mid f(x) \in R\}$.

Theorem II.2.6 (Borel, 1893)

If $f_1, \dots, f_n \in R^\times$ satisfy $f_1 + \dots + f_n = 0$ but no (non-empty) proper subset of $\{f_1, \dots, f_n\}$ sum to zero then

$$f_i/f_j \in \mathbb{C}^\times \quad \forall i, j$$

For the rest of the course, rings are commutative!

Amazing Fact: If G is a finitely generated subgroup of \mathbb{C}^\times , then for all $n \in \mathbb{N}$ the equation

$$x_1 + x_2 + \dots + x_n = 1$$

has only finitely many solutions with $x_1, \dots, x_n \in G$ in which no nonempty subset sums to zero. In fact, the number of solutions is bounded in n and in the number of generators of G . (Hard)

Extra credit: Does there exist such a G for which there exist solutions as above for infinitely many n .

From NOW ON: All rings are commutative

Example II.2.4 (Rings and Homomorphisms)

The 0 ring, $\{0\}$. For any ring R , there is a homomorphism

$$0 : R \rightarrow 0$$

$$r \mapsto 0$$

Definition II.2.6

If $f : R \rightarrow S$ is a ring homomorphism, the kernel is $\ker f := \{r \in R \mid f(r) = 0\}$.

We know from group theory that $\ker(f)$ is a normal subgroup of R (under $+$). Also, if $r \in R$ and $x \in \ker f$, then $rx \in \ker f$ because

$$f(rx) = f(r)f(x) = f(r) \cdot 0 = 0.$$

Definition II.2.7 (Ideals)

If R is a ring, an ideal of R is a subgroup of $(R, +)$ which is closed under multiplication by R .

Example II.2.5 (Ideals)

Ideals in \mathbb{Z} ? Well we know these have to be $n\mathbb{Z}$ for $n \in \mathbb{Z}_{\geq 0}$, because these are the only additive subgroups. It turns out all of these are in fact ideals.

Note: A nonempty subset of a ring R is an ideal if and only if it is closed under R -linear combinations. That is for $r_1, \dots, r_n \in R$ and $i_1, \dots, i_n \in I$ we have $\sum r_k i_k \in I$.

Definition II.2.8 (Some Ideals)

For $r \in R$, the principal ideal (r) (also denoted rR) which is $\{rr' \mid r' \in R\}$. This is of course the smallest ideal containing r .

The unit ideal of R is $(1) = 1R = R$.

The zero ideal of R is $(0) = 0R = 0$.

A “proper ideal” of R is an ideal which is not (0) or (1) .

Note: If $f : R \rightarrow S$ is a homomorphism then $\ker(f)$ is an ideal of R .

$$\ker f = (1) \iff S = 0$$

$$\ker f = (0) \iff f \text{ is injective.}$$

Definition II.2.9 (Quotient Ring)

Let R be a ring and I be an ideal. Then R/I is a group under addition. We claim that R/I is a ring, called the quotient ring.

Proof. We define

$$(r + I)(r' + I) = rr' + I.$$

Note: if $i, i' \in I$ then

$$\begin{aligned}(r+i)(r'+i') &= rr' + ri' + ir' + ii' \\ &\in rr' + I.\end{aligned}$$

Therefore we have that

$$(r+i)(r'+i') \in rr' + I$$

because additive cosets partition the set this gives $(r+i)(r'+i') + I = rr' + I$ as desired.

The rest is easy.



Example II.2.6

If $R = \mathbb{Z}$, $I = n\mathbb{Z}$, then $R/I = \mathbb{Z}/n\mathbb{Z}$, and so $\mathbb{Z}/n\mathbb{Z}$ is the quotient of the ring \mathbb{Z} by the ideal $n\mathbb{Z}$.

Definition II.2.10 (Field)

A field is a nonzero ring in which every nonzero element is a unit (i.e., has a multiplicative inverse).

Examples: $\mathbb{Q}, \mathbb{C}, \mathbb{R}, \mathbb{Z}/p\mathbb{Z}$ Non-examples: $\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}$.

Definition II.2.11 (Integral Domain)

An integral domain is a nonzero ring R such that $a, b \in R$, $ab = 0 \implies a = 0$ or $b = 0$.

If R is a field, what are the ideals of R ? Well, if $I \neq 0$ is an ideal, it contains some $i \neq 0$, so $1 = i^{-1}i \in I$. This implies that $I = (1)$. Therefore R only has (0) and (1) as its ideals.

Proposition II.2.7

If $f : R \rightarrow S$ is a ring homomorphism and R is a field, then either f is injective or $S = 0$.

Proof. Note that $\ker f$ is an ideal, and so $\ker f = (0)$ or $\ker f = (1)$. By the previous discussion this implies the result.



Notation: Often if R is a ring, I is an ideal, $r \in R$, we denote the element $r + I$ of R/I by \bar{r} .

Theorem II.2.8 (First Isomorphism)

Let $f : R \rightarrow S$ be a ring homomorphism with kernel K . Let I be some ideal of R , and let $\pi : R \rightarrow R/I$ be the quotient map. Then

(1) If $I \subseteq K$ then f uniquely factors as

$$\begin{array}{ccc} R & \xrightarrow{f} & S \\ \pi \searrow & & \nearrow \bar{f} \\ & R/I & \end{array}$$

(2) If $I = K$ then \bar{f} is injective (then if f is surjective, \bar{f} is an isomorphism).

Proof. The corresponding statements are all true for groups, so all that we need to show is that \bar{f} is a ring homomorphism.

$$\begin{aligned}\bar{f}(1 + I) &= \bar{f}(\pi(1)) = f(1) = 1 \\ \bar{f}((r + I)(r' + I)) &= \bar{f}(rr' + I)\end{aligned}$$

$$\begin{aligned}
&= \bar{f}(\pi(rr')) = f(rr') \\
&= f(r)f(r') = \bar{f}(r + I)\bar{f}(r' + I).
\end{aligned}$$

Great!



Theorem II.2.9

If $f : R \rightarrow S$ is a surjective homomorphism with kernel K , then the maps

$$\begin{aligned}
I &\mapsto f(I) \\
f^{-1}(J) &\leftarrow J
\end{aligned}$$

are inverse bijections between

$$\{\text{ideals of } R \text{ containing } K\} \leftrightarrow \{\text{ideals of } S\}$$

Proof. We know from group theory that these maps induce bijections between

$$\{\text{subgroups of } R \text{ containing } K\} \leftrightarrow \{\text{subgroups of } S\}.$$

Thus it suffices to show that if I is an ideal containing K , then $f(I)$ is an ideal, and if J is an ideal then $f^{-1}(J)$ is an ideal.

If $s \in S$, and $i \in I$, then $sf(i) = f(r)f(i) = f(ri) \in f(I)$ for some $r \in R$ by surjectivity. Thus $f(I)$ is an ideal.

Now suppose $r \in R$, $r' \in f^{-1}(J)$. Then $f(rr') = f(r)f(r') \in f(r)J \subseteq J$. Thus $rr' \in f^{-1}(J)$ as desired, and $f^{-1}(J)$ is an ideal.



Supplement: Same notation, $R/I \cong S/f(I)$ and $R/f^{-1}(J) \cong S/J$.

Proposition II.2.10

If $\varphi : R \rightarrow S$ is a surjective ring homomorphism and $I \supseteq \ker \varphi$ is an ideal of R , then $R/I \cong S/\varphi(I)$.

[Note: We showed last time that $\varphi(I)$ is indeed an ideal].

Proof. We look at the following maps

$$R \xrightarrow{\varphi} S \twoheadrightarrow S/\varphi(I).$$

Their composition is a surjective ring homomorphism, and it remains to show that the kernel is R . Well the kernel of $S \rightarrow S/\varphi(I)$ is $\varphi(I)$, and so the total kernel is $\varphi^{-1}(\varphi(I)) = I$, where equality holds by Theorem II.2.9.

Then we have from last time that

$$\begin{array}{ccc}
R & \xrightarrow{\quad} & S/\varphi(I) \\
& \searrow & \nearrow \cong \\
& R/I &
\end{array}$$

Then the induced map $R/I \rightarrow S/\varphi(I)$ is surjective and has trivial kernel. Perfect!



Example II.2.7

Compute $\mathbb{Z}[i]/(2+i)$ where $(2+i)$ denotes the “ideal generated by $2+i$.”

Formally, $\mathbb{Z}[i] \cong \mathbb{Z}[x]/(x^2+1)$. This gives us our maps

$$\mathbb{Z}[x] \xrightarrow{\varphi} \mathbb{Z}[i] \twoheadrightarrow \mathbb{Z}[i]/(2+i).$$

So what’s the preimage of $(2+i)$? Well

$$\varphi^{-1}((2+i)) = (x^2+1, 2+x).$$

So now we mod out in the other order

$$\mathbb{Z}[x] \xrightarrow{\psi} \mathbb{Z}[x]/(2+x) \cong \mathbb{Z}$$

$$f(x) \longmapsto f(-2).$$

Then by Proposition II.2.10, we see that

$$\begin{aligned} \mathbb{Z}[i]/(2+i) &\cong \mathbb{Z}[x]/(x^2+1, 2+x) \\ &\cong \mathbb{Z}/((-2)^2+1) = \mathbb{Z}/5\mathbb{Z}. \end{aligned}$$

Idea: The “free” ring on one generator x is exactly $\mathbb{Z}[x]$. This idea carries us forward in many ways by using “universal” maps such as $\mathbb{Z}[x] \rightarrow \mathbb{Z}[i]$ as above. This is nice because $\mathbb{Z}[x]$ is nice (e.g. it has unique prime factorization).

Summary: Polynomial rings $\mathbb{Z}[x_1, \dots, x_n]$ play the role for (commutative) rings that free groups play for groups—namely, every ring R with generators g_1, \dots, g_n is the homomorphic image of

$$\begin{aligned} \mathbb{Z}[x_1, \dots, x_n] &\rightarrow R \\ f(x_1, \dots, x_n) &\mapsto f(g_1, \dots, g_n) \\ \sum_{\bar{\ell}=(\ell_1, \dots, \ell_n)} a_{\bar{\ell}} x^{\bar{\ell}} &\mapsto \sum_{\bar{\ell}} a_{\bar{\ell}} g_1^{\ell_1} \cdots g_n^{\ell_n} \end{aligned}$$

II.3. Polynomial Rings**Definition II.3.1**

Let R be a ring. Then $R[X]$ is defined as

$$R[X] := \left\{ \sum_{i=0}^n a_i X^i \mid n \in \mathbb{N}, a_i \in R \right\}.$$

Addition and multiplication are as usual for polynomials. Namely

$$\sum_{i=0}^n a_i X^i + \sum_{j=0}^m b_j X^j = \sum_{k=0}^{\max(n,m)} (a_k + b_k) X^k$$

where $a_k, b_k = 0$ if $k > n, k > m$ respectively. Furthermore

$$\left(\sum_{i=0}^n a_i X^i \right) \left(\sum_{j=0}^m b_j X^j \right) = \sum_{k=0}^{m+n} \left(\sum_{\ell=0}^k a_{\ell} b_{k-\ell} \right) X^k$$

with the same conventions.

One could do $R[X_1, \dots, X_k]$ similarly.

Definition II.3.2

For $f(X) = \sum_{i=0}^n a_i X^i \in R[X]$ the degree $\deg f(X)$ of $f(X)$ is the largest i such that $a_i \neq 0$ if such an i exists (otherwise $f(X) = 0$, and $\deg f = -\infty$).

If $f(X) \neq 0$, the leading coefficient of f is $a_{\deg f}$. We say $f(X) \neq 0$ is monic if $a_{\deg f} = 1$.

Fact: For $f, g \in R[X]$, we have that

$$\deg(fg) \leq \deg(f) + \deg(g)$$

with equality if R is an integral domain (this implies that if R is an integral domain then $R[X]$ is an integral domain). Furthermore

$$\deg(f + g) \leq \max(\deg f, \deg g)$$

with equality when $\deg(f) \neq \deg(g)$.

Definition II.3.3

For any ring R and any $r \in R$, there is a unique ring homomorphism

$$\text{ev}_r : R[X] \rightarrow R$$

mapping $X \mapsto r$ and $s \mapsto s$ for all $s \in R$. Namely $f(X) \mapsto f(r)$. This is called evaluation at r .

More generally, if $\varphi : R \rightarrow S$ is a ring homomorphism and $s \in S$, there exists a unique homomorphism $\tilde{\varphi} : R[X] \rightarrow S$ mapping $X \mapsto s, r \mapsto \varphi(r)$. Namely

$$\tilde{\varphi} : \sum_{i=0}^n a_i X^i \mapsto \varphi(a_i) s^i.$$

Proof of uniqueness. DIY!



Example II.3.1

Let $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}/5\mathbb{Z} \hookrightarrow (\mathbb{Z}/5\mathbb{Z})[X]$. Then we get

$$\tilde{\varphi} : \mathbb{Z}[X] \rightarrow (\mathbb{Z}/5\mathbb{Z})[X]$$

All of this works for multivariable polynomials too (with notions of degree with respect to a variable and total degree).

Note that: $R[X, Y] \cong (R[X])[Y] \cong (R[Y])[X]$, which we just identify.

Theorem II.3.1 (Polynomial Division Algorithm)

Given $f(X), g(X) \in R[X]$ where $g(X) \neq 0$ is monic, then there exists a unique $q(X), r(X) \in R[X]$ such that

$$f(X) = g(X)q(X) + r(X)$$

and $\deg r < \deg g$.

Proof. Existence: say $\deg g = m$. If $n \geq m$, then $X^n = X^{n-m}g(X) + h(X)$ where $\deg h < n$. Why? Well write $g(X) = \sum_{i=0}^m b_i X^i$. Then

$$X^n = X^{n-m}g(X) - \sum_{i=0}^{m-1} b_i X^{n-m+i}.$$

Similarly, if $c(X)$ has degree $n \geq m$ and leading coefficient a , then

$$c(X) = aX^{n-m}g(X) + h(X)$$

with $\deg(h) < \deg c$.


Repeat this, replacing c by h , and continue to get $f = gq + r$, with $\deg r < \deg g$.

Uniqueness: Suppose $f = gq + r = g\tilde{q} + \tilde{r}$ with $\deg r, \deg \tilde{r} < \deg g$. Then

$$r - \tilde{r} = g(\tilde{q} - q).$$

But we know that because g is monic

$$\deg(r - \tilde{r}) < \deg g \quad \deg(g(q - \tilde{q})) = \deg g + \deg(q - \tilde{q}).$$

Together this forces $\deg(q - \tilde{q}) = -\infty$, so $q = \tilde{q}$, and $r = \tilde{r}$ by plugging into the equation above. Perfect! 

Corollary II.3.2

If K is a field (that is a ring with $K^\times = K \setminus \{0\}$), then $K[X]$ admits a Euclidean algorithm (which implies unique prime factorization).


The proof will be held until later until after we define things.

Lemma II.3.3

For any ring R , there exists a unique (ring) homomorphism $\varphi : \mathbb{Z} \rightarrow R$.

For $n \in \mathbb{Z}$, we'll write n (in R) for $\varphi(n)$.

Proof. Uniqueness: We know $\varphi(1) = 1_R$, and then $\varphi(n) = 1_R + \cdots + 1_R$, n times (or with negatives in the appropriate cases). This gives a unique formula for φ .

Existence: It is then easy to check that this formula gives a ring homomorphism. 

Definition II.3.4

If R is a ring with $\varphi : \mathbb{Z} \rightarrow R$, then we know that $\ker \varphi$ is an ideal of \mathbb{Z} . But then $\ker \varphi = m\mathbb{Z}$ for some unique $m \in \mathbb{Z}_{\geq 0}$.

Here m is the order of 1_R under addition if 1_R has finite order, and 0 otherwise. We call m the characteristic of R .

Example II.3.2

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{Z}[i]$ have characteristic 0. $\mathbb{Z}/3\mathbb{Z}, (\mathbb{Z}/3\mathbb{Z})[X]$ has characteristic 3. Also $\mathbb{Z}[i]/(2+i)$ has characteristic 5.

Definition II.3.5

In any ring R , an element $r \in R$ is called irreducible if all three of the following conditions hold

- $r \neq 0$
- r is not a unit in R
- r is not the product of two non-units in R .

Definition II.3.6

We say that R is a unique factorization ring if every $r \neq 0$ which is not a unit can be written as a product $\prod_{i=1}^n f_i$ where $f_i \in R$ is irreducible. In addition, if $\prod_{i=1}^n f_i = \prod_{j=1}^m g_j$ with $f_i, g_j \in R$ irreducible, then $n = m$ and there is some permutation $\sigma \in S_n$ such that f_i is a unit times $g_{\sigma(i)}$ for all i .

Last time: If R is a ring, $f, g \in R[x]$ with $g \neq 0$ and the leading coefficient of g a unit in R , then $f = gq + r$ for some $q, r \in R[x]$ with $\deg r < \deg g$.

Corollary II.3.4

For $\alpha \in R$ and $f(x) \in R[x]$, there exists $q(x) \in R[x]$ and $c \in R$ such that

$$f(x) = (x - \alpha)q(x) + c.$$

If we evaluate at α , we then see that $c = f(\alpha)$.

Example II.3.3

Look at $4x^3 + x$ in $\mathbb{Z}[x]$. Then we see that

$$4x^3 + x = (2x)(2x^2) + x$$

But $4x^3 + x \neq (2x)q(x) + r(x)$ where $\deg(r) < \deg(2x) = 1$.

If K is a field, what are the ideals in $K[x]$?

Definition II.3.7 (Principal Ideal)

In a ring R , for any $\alpha \in R$, $(\alpha) := \alpha R$ is called a principal ideal. Note that $(\alpha) = (\alpha u)$ for any $u \in R^\times$.

A principal ideal domain is an integral domain R where every ideal is principal.

Proposition II.3.5


Let K be a field. Any nonzero ideal I in $K[x]$ is $(g(x))$ where $g(x) \neq 0$ is any element of I having the smallest possible degree.

This shows that $K[x]$ is a principal ideal domain.

Proof. Fix some nonzero $g(x) \in I$ having the smallest possible degree. Now for $f(x) \in I$, we see that

$$f = gq + r$$

where $g, r \in K[x]$ and $\deg r < \deg g$. But then $r = f - gq \in I$, so the minimality of $\deg g$ implies that $r = 0$.

Perfect! This shows us that $f \in (g)$. The other inclusion $(g) \subseteq I$ is trivial. 

Proposition II.3.6


If R is an integral domain, $\alpha, \beta \in R$ then $(\alpha) = (\beta)$ if and only if $\alpha = \beta u$ for $u \in R^\times$.

Proof. We have $(\alpha) = (\beta)$ if and only if $\alpha = \beta x, \beta = \alpha y$ for some $x, y \in R$.

Then we see that

$$\alpha = \beta x = \alpha y x$$

$$\alpha(1 - yx) = 0$$

so either $\alpha = 0$, implying $\beta = 0$ so $\alpha = \beta \cdot 1$. Otherwise $yx = 1$, in which case $x, y \in R^\times$ and we have that $\alpha = \beta x$. 

Example II.3.4

If R is an integral domain, then $(R[x])^\times = R^\times$.

If $R = \mathbb{Z}/4\mathbb{Z}$, we have that $(R[x])^\times = 1 + 2R[x]$. This happens because if $f \in R[x]$ then

$$(2f + 1)^2 = 4f^2 + 4f + 1 = 1.$$

If $f, g \in R[x]$ satisfy $fg = 1$, then apply $\varphi : R[x] \rightarrow (R/(2))[x]$ to get $\varphi(f)\varphi(g) = 1$.

Therefore $\varphi(f) = \varphi(g) = 1$. Thus $f = 1 + 2A, g = 1 + 2B$ for $A, B \in R[x]$. Then

$$fg = 1 + 2(A + B) + 4AB = 1 + 2(A + B)$$

which is 1 if and only if $A = B + 2C$, Thus

$$f = 1 + 2(B + 2C) = 1 + 2B = g.$$

If $R = \mathbb{Z}/6\mathbb{Z}$, we have that $(\mathbb{Z}/(6)[x])^\times = \{\pm 1\}$.

Definition II.3.8 (Product Ring)

If R, S are rings, then $R \times S$ with coordinate wise addition/multiplication is a “product ring.”

II.4. Ring Extensions

Example II.4.1

We want to think of things like

$$\mathbb{Z}[i] = \mathbb{Z}[x]/(x^2 + 1)$$

and i is the image of x in this ring. We also have

$$\mathbb{Z}[1/2] = \mathbb{Z}[x]/(2x - 1)$$

If R is a ring, and I is an ideal of $R[x]$, then we can consider $R[x]/I$. This is obviously a ring, and there is a homomorphism $R \rightarrow R[x] \rightarrow R[x]/I$. This homomorphism might not be injective

Definition II.4.1 (Ring Extension)

If R is a ring and I is an ideal of $R[x]$, then we say that $R[x]/I$ is an extension of R provided that the homomorphism $R \rightarrow R[x]/I$ is injective.

Example II.4.2

Consider $(\mathbb{Z}/4\mathbb{Z})[x]/(2x - 1)$. Let u be the image of x in this ring. Then we see that

$$2u = 1 \implies 4u^2 = 1 \implies 0 = 1.$$

Definition II.4.2 (Module)

A module M over a ring R is an abelian group M equipped with a map $R \times M \rightarrow M$ satisfying

- $1 \cdot x = x$
- $(a + b)x = ax + bx$.
- $a(x + y) = ax + ay$.
- $a(bx) = (ab)x$.

Intuitively these are the same as vector spaces, but the scalars can come from a ring instead of from a field.

Example II.4.3

If $f(x) \in R[x]$ is a monic polynomial of degree n , then $S := R[x]/(f(x))$ is an extension of R . For convenience let u be the image of x in S .

Then each element of S can be written in exactly one way as $a(x) + ((f(x)))$ with $\deg(a) < n$ since if $g(x) \in R[x]$ then $g = fq + r$ for some unique $q, r \in R[x]$ with $\deg r < n$.

This means that S is a “free” R -module of dimension n . That is we have a basis $1, u, u^2, \dots, u^{n-1}$ for S .

Definition II.4.3

Let R be a principal ideal domain, so for $f, g \in R$, we know $(f, g) = (h)$ for some $h \in R$.

Thus $h = uf + vg$ for some $u, v \in R$ and $f = hr, g = hs$ for some $r, s \in R$.

This shows that h is a greatest common divisor of f, g . Namely if $w \in R$ divides both f, g , then $w \mid uf + vg = h$.

Proposition II.4.1

Every principal ideal domain is a unique factorization domain

Proof. Using the proof for \mathbb{Z} , for uniqueness it suffices to show that if $p \in R$ is irreducible and $p \mid fg$, then $p \mid f$ or $p \mid g$.

If $p \nmid f$, then $(p, f) = (h)$ for some $h \in R$. Because $h \mid p$ and p is irreducible, we know that h is a unit or h is a unit times p . However because $p \nmid f$, we know h is not p times a unit. Therefore we can assume $h = 1$ because $(h) = (1)$.

Therefore $pu + fv = 1$ for some $u, v \in R$. Multiplying by g we see that $pug + fgv = g$. We know that $p \mid fg$ by hypothesis, so this shows that $p \mid g$ as desired.

We will do existence later! See Proposition II.6.6

**Example II.4.4**

If K is a field then $K[x]$ is a principal ideal domain and thus a unique factorization domain.

The proof for existence is not difficult in $K[x]$ (DIY!)

Extra Credit Problem on HW2 extended until Thursday night.

Theorem II.4.2

If R is an integral domain, then there exists an injective homomorphism $\varphi : R \hookrightarrow K$ for some field K .

More precisely, there is a field $\text{Frac}(R)$ which is in some sense the “smallest field” with such an injective map $R \hookrightarrow \text{Frac}(R)$. This field is called the field of fractions of R , or the fraction field of R .

That is for every $\varphi : R \hookrightarrow K$, there exists a unique map $\text{Frac}(R) \hookrightarrow K$ such that the following diagram commutes

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & K \\ & \searrow & \nearrow \\ & \text{Frac}(R) & \end{array}$$

Proof. Let $\text{Frac}(R) = \{(a, b) \mid a, b \in R, b \neq 0\} / \sim$. Defining $(a, b) \sim (c, d) \iff ad = bc$.

Then we write a/b for the equivalence class of (a, b) . Then define

$$\begin{aligned} \frac{a}{b} + \frac{c}{d} &:= \frac{ad + bc}{bd} \\ \frac{a}{b} \cdot \frac{c}{d} &:= \frac{ac}{bd}. \end{aligned}$$

We check that these are well-defined. Namely say $a/b = A/B$ and $c/d = C/D$. We must check

$$\begin{aligned} \frac{ad + bc}{bd} &= \frac{AD + BC}{BD} \\ \frac{ac}{bd} &= \frac{AC}{BD} \end{aligned}$$

To check this we see that

$$\begin{aligned} BD(ad + bc) &= BaDd + BbDc = bADd + BbdC \\ &= bd(AD + BC) \\ acBD &= AbCd = ACbd. \end{aligned}$$

It is not difficult to check that $\text{Frac}(R)$ is a field. and $R \hookrightarrow \text{Frac}(R)$ by $r \mapsto r/1$. Also $(a/b)^{-1} = b/a$ if $a \neq 0$.

The mapping property is also not difficult to verify, because we can define $a/b = ab^{-1} \mapsto \varphi(a)\varphi(b)^{-1}$. 🍷

Example II.4.5

$\text{Frac}(\mathbb{Z}) = \mathbb{Q}$. If K is a field then $\text{Frac}(K[X]) = K(X)$ (the rational functions, ratios of polynomials).

Also $\mathbb{Z}[X] = \mathbb{Q}(X)$.

Example II.4.6

We have that

$$\frac{\mathbb{C}[x, y]}{(xy - 1)} = \mathbb{C}[x, 1/x]$$

II.5. Basic Algebraic Geometry

Definition II.5.1 (Maximal Ideal)

A maximal ideal M of a ring R is an ideal $M \neq R$ such that there does not exist an ideal I such that $M \subsetneq I \subsetneq R$.

Example II.5.1

If $R = \mathbb{Z}$, the maximal ideals are $p\mathbb{Z}$ for p a prime.

If $R = \mathbb{C}[X]$, the maximal ideals are $(X - \alpha)$ for $\alpha \in \mathbb{C}$.

Intuitively this means that the maximal ideals are points in \mathbb{C} , and we should think of the maximal ideals in \mathbb{Z} as “points” in some space. See homework for the definition of $\text{Spec } R$.

Lemma II.5.1

If $\varphi : R \rightarrow S$ is a surjective ring homomorphism, then $\ker(\varphi)$ is a maximal ideal if and only if S is a field.

Proof. Use the correspondence theorem (see Theorem II.2.9). This means that

$$\begin{aligned} \ker \varphi \text{ is maximal} &\iff \text{the only ideals of } R \text{ containing} \\ &\ker \varphi \text{ are } (1) \text{ and } \ker(\varphi) \text{ and } \ker(\varphi) \neq (1) \\ &\stackrel{\text{Cor}}{\iff} \text{the only ideals of } S \text{ are } (0), (1), (0) \neq (1) \\ &\iff S \text{ is a field.} \end{aligned}$$

**Corollary II.5.2**

An ideal I of R is maximal if and only if R/I is a field.

Corollary II.5.3

The ideal (0) of R is maximal if and only if R is a field.

Lemma II.5.4

If K is a field, then

- (1) The maximal ideals of $K[X]$ are exactly (f) for irreducible $f \in K[X]$. (DIY, use that $K[X]$ is principal)
- (2) If $\varphi : K[X] \rightarrow S$ is a homomorphism to an integral domain S , then $\ker \varphi$ is either (0) or a maximal ideal.

Proof of (2). Note that if $fg \in \ker \varphi$, this implies $\varphi(f)\varphi(g) = 0$, so $\varphi(f) = 0$ or $\varphi(g) = 0$. thus $f \in \ker \varphi$ or $g \in \ker \varphi$.

But note that $\ker \varphi$ is an ideal of $K[X]$, so it must be (h) for some h . We then use the fact that $K[X]$ is an integral domain to show that $h = 0$, h is irreducible, or (1) .

But then (1) is ruled out by the fact that S is an integral domain.

**Theorem II.5.5** (Hilbert's Nullstellensatz)

The maximal ideals of $R := \mathbb{C}[X_1, \dots, X_n]$ are in “natural” bijection with the points in \mathbb{C}^n . Explicitly they are

$$(X_1 - \alpha_1, \dots, X_n - \alpha_n)$$

with $\alpha_1, \dots, \alpha_n \in \mathbb{C}$.

Proof. Note this ideal is the kernel of the evaluation map $\mathbb{C}[X_1, \dots, X_n] \rightarrow \mathbb{C}$ taking X_i to α_i . This is surjective, and so the kernel is a maximal ideal.

We now prove the converse. Let M be a maximal ideal of R . Then we have a quotient map $R \twoheadrightarrow R/M$, and R/M is a field.

Restrict to the subring $\mathbb{C}[X_i] \hookrightarrow R \twoheadrightarrow R/M$. Then we have a ring homomorphism $\mathbb{C}[X_i] \rightarrow R/M$. Because R/M is an integral domain, Lemma II.5.4 tells us that $\mathbb{C}[X_i] \rightarrow R/M$ is either (0) or a maximal ideal of $\mathbb{C}[X_i]$.

In fact we have either (0) or $(X_i - \alpha_i)$ as the ideal for some constant α_i because \mathbb{C} is algebraically closed. But it can't be (0), since if it were (0), then $\mathbb{C}(X_1)$ would embed into R/M (by Theorem II.4.2).

But these maps are necessarily the identity on \mathbb{C} , but then a vector space of uncountable dimension embedding into a vector space of countable dimension (all over \mathbb{C}). This is impossible. Explicitly $\mathbb{C}[x_1, \dots, x_n]$ is spanned by $x_1^{e_1} \cdots x_n^{e_n}$ for $e_1, \dots, e_n \in \mathbb{Z}_{\geq 0}$. Then $\mathbb{C}(X)$ has an uncountable collection of independent vectors

$$\frac{1}{X - \alpha}, \alpha \in \mathbb{C}.$$

We conclude $\mathbb{C}[X_i] \hookrightarrow R \twoheadrightarrow R/M$ has kernel $(X_i - \alpha_i)$. Thus M contains $(X_i - \alpha_i)$, and so

$$(X_1 - \alpha_1, \dots, X_n - \alpha_n) \subseteq M \not\subseteq (1).$$

By maximality we get the desired equality. 

Corollary II.5.6


If I is an ideal of $\mathbb{C}[X_1, \dots, X_n]$ generated by some f_1, \dots, f_k , and $V(I)$ is the set of all

$$\alpha := (\alpha_1, \dots, \alpha_n) \in \mathbb{C}^n \text{ such that } f_i(\alpha) = 0. \quad \forall i$$

Then the maximal ideals of R/I are in bijection with $V(I)$.

Proof. The maximal ideals of R/I are given by $\pi(M)$ where M is any maximal ideal of R which contain I . This is in fact a bijection.

Well $I \subseteq M$ means that $f_1, \dots, f_k \in M$. Thus M is maximal if and only if $M = (X_1 - \alpha_1, \dots, X_n - \alpha_n)$.

We know $f_i \in M$ if and only if f_i is in the kernel of $f \mapsto f(\alpha_1, \dots, \alpha_n)$. That is if and only if $(\alpha_1, \dots, \alpha_n) \in V(I)$. 

Lemma II.5.7 (Zorn's Lemma)

If S is a partially ordered set in which every totally ordered subset has an upper bound, then every subset has an upper bound.


Corollary II.5.8

If R is a ring and $I \neq (1)$ is an ideal, then I is contained in a maximal ideal.

Proof. Let S be the set of ideals containing I which aren't (1). This is a partially ordered set under containment. If T is a totally ordered subset of S , then we claim the ideal J which is the union of all ideals in T .

This is an ideal since if we have a finite linear combination $\sum_i r_i j_i$ for $j_i \in T_i \in T$, then there is some n so that $T_i \subseteq T_n$ by total ordering. And then $\sum_i r_i j_i \in T_n$.

If we have $1 \in J$ then we would have 1 lying in some ideal lying in T , which is impossible.


Then by Zorn's Lemma, S contains a maximal element, which is a maximal ideal containing I . 

Corollary II.5.9

If a ring R has no maximal ideals, then R is the zero ring.

Corollary II.5.10

$f_1, \dots, f_k \in \mathbb{C}[x_1, \dots, x_n]$ have no common zeros if and only if $(f_1, \dots, f_k) = (1)$. That is $1 = \sum_i g_i f_i$ for some $g_i \in \mathbb{C}[x_1, \dots, x_n]$.

Proof. The converse is obvious. To show the forward direction (by contrapositive), note that if (f_1, \dots, f_k) is not (1), then (f_1, \dots, f_k) is contained in a maximal ideal $(X_1 - \alpha_1, \dots, X_n - \alpha_n)$ where $\alpha_i \in \mathbb{C}$. Then f_i are all zero on $\alpha = (\alpha_1, \dots, \alpha_n)$. 

Theorem II.5.11 (Bézout's Theorem)

If $f(X, Y)$ and $g(X, Y)$ are polynomials in $\mathbb{C}[X, Y]$ with no (nonconstant) common factor, then they only have finitely many common zeroes.

(In fact, we won't show this but the number of zeroes is at most the product of their total degrees).

Proof. We know $\mathbb{C}[X, Y] = (\mathbb{C}[Y])[X] \subseteq (\mathbb{C}(Y))[X]$.

The ideal (f, g) in $(\mathbb{C}(Y))[X]$ is principal, say it's (h) where $h \in (\mathbb{C}(Y))[X]$. For the sake of contradiction, suppose $(h) \neq (1)$. Note that $h = v(y)h_1(x, y)/u(y)$ where $h_1 \in \mathbb{C}[X, Y]$, $v, u \in \mathbb{C}[y] \setminus \{0\}$ (we know $v \neq 0$ because at least one of f, g is nonzero).

But $v(y)/u(y)$ is a unit so $(h) = (h_1)$ in this ring. Thus we may assume $h \in \mathbb{C}[X, Y]$ with no $\mathbb{C}[y]$ dividing h . For some $r, s \in (\mathbb{C}(Y))[X]$ we then have

$$rf + sg = h.$$

Then clearing denominators, we have $r_1, s_1 \in \mathbb{C}[X, Y]$ and $u \in \mathbb{C}[Y] \setminus \{0\}$ such that

$$r_1 f + s_1 g = hu$$

and we may assume u, r, s have no common factors. If $h = 1$, then any common root (x_0, y_0) of f, g would have $u(y_0) = 0$. Thus there are finitely many possibilities for y_0 , and similarly we can show there are finitely many possibilities for x_0 .

Now we show h is a unit multiple of one. We know that $h \mid f$ in $(\mathbb{C}(y))[x]$. This says that

$$h \frac{a(y)}{b(y)} H(x, y) = f$$


where $a, b \in \mathbb{C}[y]$ are coprime, $b \neq 0$, with $H(x, y) \in \mathbb{C}[x, y]$ not divisible by any nonconstant polynomial in $\mathbb{C}[Y]$. Then

$$h(x, y)a(y)H(x, y) = b(y)f(x, y).$$

If $b(y)$ is nonconstant, then it has a root $\beta \in \mathbb{C}$. Then

$$h(x, \beta)a(\beta)H(x, \beta) = 0.$$

Thus $y - \beta$ divides one of h, a, H . It cannot divide a because a, b are coprime. It cannot divide h or H because no nonconstant polynomial in $\mathbb{C}[Y]$ divides h, H . Therefore b is constant, and we see that $h \mid f$ in $\mathbb{C}[X, Y]$

Similarly, $h \mid g$ in $\mathbb{C}[X, Y]$. This is a contradiction unless h is a nonzero constant, that is a unit multiple of one. This finishes the proof! 

II.6. Euclidean Domains, PIDs, Noetherian-ness, and UFDs

If R is an integral domain, then

$$u \in R^\times \iff (u) = (1).$$

And we have a condition for when u is irreducible (i.e, $u \neq 0$, u is not a unit, and u is not a product of two nonzero non-units). Namely

$$r \text{ is irreducible} \iff (0) \subsetneq (r) \subsetneq (1) \text{ is maximal among principal ideals}$$

$$r \text{ is reducible} \iff (0) \subsetneq (r) \subsetneq (a) \subsetneq (1) \text{ for some } a \in R.$$

Definition II.6.1


We say that $r \in R$ is prime provided that r is not a unit and when $r \mid ab$ we have $r \mid a$ or $r \mid b$.

Lemma II.6.1

If R is an integral domain and $r \in R$ is prime and $r \neq 0$, then r is irreducible

Proof. Let $r = ab$ where a, b are nonzero. Thus $r \mid ab$, so $r \mid a$ or $r \mid b$. If $r \mid a$ then

$$a = rs \implies r = rsb \implies r(1 - sb) = 0.$$

for some $s \in R$. By cancellation (within an integral domain), $sb = 1$, so b is a unit. Great! This shows either a, b are a unit. Thus r is irreducible. 

Lemma II.6.2

If R is a principal ideal domain and $r \in R$ is irreducible, then r is prime.

Proof. Suppose that $r \mid ab$. Then $(r, a) = (h)$ for some $h \in R$. Thus $h \mid r$. If h is not a unit, then $r = h \cdot \text{unit}$, meaning that $(r) = (h)$. This means that $r \mid a$.

So suppose h is a unit. Then $rx + ry = 1$ for some $x, y \in R$. Therefore

$$rbx + aby = b$$

and since $r \mid ab$ we see that $r \mid b$. Perfect!



Note: In an integral domain, if $r \in R$ is prime, then $r \mid a_1 a_2 \cdots a_k$ implies $r \mid a_i$ for some i . If in addition all a_i are irreducible, then $r = a_i \cdot \text{unit}$ for some i .

Lemma II.6.3

If R is an integral domain in which all irreducible elements are prime, then any nonzero element of R has at most one prime factorization (up to equivalence).

I.e., if $p_1 \cdots p_k = q_1 \cdots q_\ell$ with p_i, q_j prime in R , then $k = \ell$ and there is some $\sigma \in S_k$ such that $p_i = q_{\sigma(i)} \cdot \text{unit}$ for all i .

Proof. If $p_1 \cdots p_k = q_1 \cdots q_\ell$ for p_i, q_j irreducible, then $p_1 \mid q_1 \cdots q_\ell$.

Thus $p_1 = q_j \cdot \text{unit}$ for some j . We can then just cancel and induct on the length. Namely

$$p_2 \cdots p_k = \left(\prod_{r \neq j} q_r \right) \cdot \text{unit}$$



Next Time: If R is a PID (or more generally, if every ideal in R is finitely generated) then every nonzero non-unit in R admits a factorization into irreducibles.

This shows that if R is a PID, then R is a UFD (see Proposition II.4.1).

Definition II.6.2

An integral domain R is Euclidean if there exists a map $\phi : R \rightarrow \{-\infty\} \cup \mathbb{Z}_{\geq 0}$ such that for all $a, b \in R$ with $b \neq 0$ there exists $q, r \in R$ such that $a = bq + r$ where $\phi(r) < \phi(b)$.

Example II.6.1

$R = \mathbb{Z}$, $\phi(n) = |n|$. If $R = K[x]$ for K a field, then $\phi(f) = \deg(f)$.

Lemma II.6.4

$\mathbb{Z}[i]$ is Euclidean with $\phi(x) = |x|^2$, that is $\phi(a + bi) = a^2 + b^2$.

Proof. Given $a, b \in \mathbb{Z}[i]$, $b \neq 0$, we want $q, r \in \mathbb{Z}[i]$ such that $a = bq + r$ and $|r| < |b|$.

Well, this is equivalent to saying $a/b = q + r/b$ where $|r/b| < 1$. Well clearly for all $\alpha \in \mathbb{C}$ there exists a $q \in \mathbb{Z}[i]$ such that $\alpha - q = u + vi$ where $u, v \in \mathbb{R}$, $|u|, |v| \leq 1/2$.

Furthermore if $\alpha \in \mathbb{Q}[i]$ then $u, v \in \mathbb{Q}$. Well then $|\alpha - q| \leq \sqrt{1/2} < 1$. Then we can just write $r = b(u + vi)$. We know then that $r = a - bq \in \mathbb{Z}[i]$, and $|r| < |b|$.



Definition II.6.3

A ring R is Noetherian provided that every ideal is finitely generated.

Proposition II.6.5

If a ring R is Noetherian if and only if there is no infinite ascending chain of ideals


$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$$

This is called the ascending chain condition.

Proof. Suppose R is Noetherian and that we have such an ascending chain. Then $\bigcup_n I_n$ is finitely generated. Each generator is in I_n for some n , so then all generators are in I_N for some N . Thus $\bigcup_n I_n = I_N$. This is a contradiction as it implies $I_N = I_{N+1}$.

Suppose R satisfies the ascending chain condition. Now fix some ideal I , and suppose it is not finitely generated. Then we can select elements $r_1, r_2, \dots \in I$ so that

$$(r_1) \subsetneq (r_1, r_2) \subsetneq (r_1, r_2, r_3) \subsetneq \dots \subseteq I.$$

But this contradicts the ascending chain condition. 

Proposition II.6.6

If R is Noetherian integral domain, then every nonzero nonunit in R is a product of irreducible elements.

Proof. Suppose otherwise. Then there exists an $x \in R$ which is nonzero, non-unit, and not a product of irreducibles.

Then x is reducible, say $x = yz$. At least one of y or z is neither a unit nor a product of irreducibles. Then write $x = x_1 y_1$, where x_1 is not a unit or a product of irreducibles and y_1 is not a unit.

Repeat this process, writing $x_n = x_{n+1} y_{n+1}$ where x_{n+1} is not a unit nor a product of irreducibles and y_{n+1} is not a unit.

Since y_{n+1} is not a unit we have

$$(x) \subsetneq (x_1) \subsetneq (x_2) \subsetneq (x_3) \subsetneq \dots$$

This contradicts the ascending chain condition (see Proposition II.6.5). 

Last time

$$R = \text{PID} \implies \text{all irr. are prime} \implies \text{every elt of } R \text{ has at most one factorization into irr.}$$

And this time

$$R = \text{PID} \implies R = \text{Noetherian} \implies \text{every elt of } R \text{ has some factorization into irr.}$$

Therefore we have

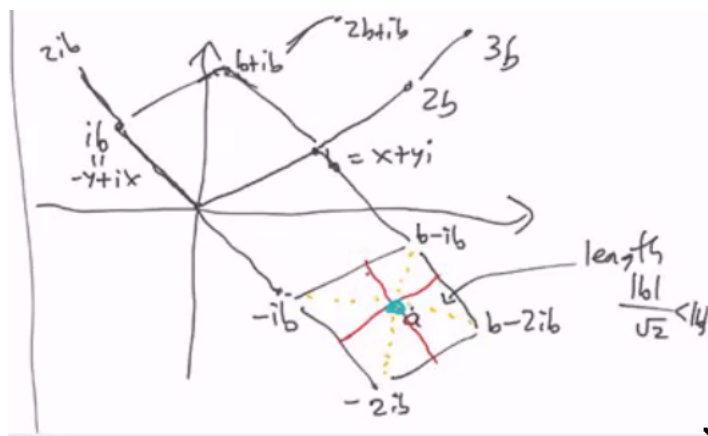
$$R = \text{PID} \implies R = \text{UFD}$$

Lemma II.6.7

If R is a Euclidean integral domain then R is a PID.

Proof. Let $\phi : R \rightarrow \{-\infty\} \cup \mathbb{Z}_{\geq 0}$ be a Euclidean function on R .

If I is a nonzero ideal of R , then $\emptyset \neq \phi(I \setminus \{0\}) \subseteq \{-\infty\} \cup \mathbb{Z}_{\geq 0}$. Then $\phi(I \setminus \{0\})$ has a smallest element $\phi(b)$ for $b \in I \setminus \{0\}$. We claim that $I = (b)$.

FIGURE 1. $\mathbb{Z}[i]$ is Euclidean

Clearly $(b) \subseteq I$. Suppose $a \in I$. Then $a = bq + r$ for some r with $q, r \in R$, and $\phi(r) < \phi(b)$. Thus $r = a - bq \in I$. Therefore $r = 0$ by minimality of $\phi(b)$. This shows that $a = bq \in (b)$.

Perfect! 

Example II.6.2

$\mathbb{Z}[i]$ is Euclidean with $\phi(x + iy) = x^2 + y^2 = |x + iy|^2$. One can see this by thinking of the picture Figure 1 with $b = x + yi$.

Namely, this picture shows us that any element of $\mathbb{Z}[i]$ lies within one of these squares, and then we can approximate by one of the corners of the squares, with an r remainder term.

Example II.6.3

But $\phi(a + b\sqrt{-3}) = a^2 + 3b^2$ is NOT a Euclidean function on $\mathbb{Z}[\sqrt{-3}]$ since you can't divide $1 + \sqrt{-3}$ by 2 to get a smaller remainder.

Moreover, $\mathbb{Z}[\sqrt{-3}]$ is not Euclidean, since it's not a UFD. Namely $(1 + \sqrt{3})(1 - \sqrt{3}) = 4 = 2 \cdot 2$. It is not difficult to show these are all irreducible and they're not unit multiples of each other.

But $\mathbb{Z}[(1 + \sqrt{-3})/2]$ is Euclidean with ϕ as a Euclidean function.

We know $\mathbb{Z}[i]$ is Euclidean. What are the primes in $\mathbb{Z}[i]$? Well we know it has a Euclidean function called the "norm"

$$N : \mathbb{Z}[i] \rightarrow \mathbb{Z}$$

$$a + bi \mapsto a^2 + b^2 = |a + bi|^2.$$

Then $N(xy) = N(x)N(y)$. And also $N(x) = x\bar{x}$ where $\overline{a + bi} = a - bi$.

Lemma II.6.8

We have the following in $\mathbb{Z}[i]$


$$N(x) \geq 0$$

$$N(x) = 0 \iff x = 0$$

$$N(x) = 1 \iff x = \pm 1, \pm i$$

$$N(x) = 1 \iff x \text{ is a unit}$$

Proof. The first three statements are nearly trivial. For the other direction, if $N(x) = 1$ then $x\bar{x} = 1$, so x is a unit.

If x is a unit, then $xy = 1$ for some y , so $N(xy) = N(1) = 1$. By multiplicativity, we have $N(x)N(y) = 1$. Since $N(x), N(y)$ are integers, $N(x) = 1$. 

Corollary II.6.9

If $x \in \mathbb{Z}[i]$ and $N(x)$ is prime in \mathbb{Z} , then x is irreducible in $\mathbb{Z}[i]$.

But there are other irreducibles in $\mathbb{Z}[i]$ too!

Given $x \in R$ which is non-zero, non-unit, then $N(x) = \mathbb{Z}_{\geq 2}$. If x is irreducible, then \bar{x} is irreducible. So $N(x)$ is a product of two irreducibles in $\mathbb{Z}[i]$.

But $N(x)$ can also be factored as $N(x) = p_1 \cdots p_k$ prime numbers in \mathbb{Z} . Then we write each p_i as a product of irreducibles in $\mathbb{Z}[i]$. So either $k = 1$ and p_1 is a product of two irreducibles in $\mathbb{Z}[i]$. Or $k = 2$ and p_1, p_2 are each irreducible in $\mathbb{Z}[i]$ where $x = up_1, \bar{x} = vp_2$ implying $p_1 = p_2$ for $u, v \in \{\pm 1, \pm i\}$.

It remains to show that for $p \in \mathbb{Z}$ prime

$$p \text{ is irreducible in } \mathbb{Z}[i] \iff p \equiv 3 \pmod{4}.$$

We'll do this next time!

Midterm: Monday February 21st (13 days from now).


We know $\mathbb{Z}[i]$ is Euclidean \implies PID \implies UFD

Lemma II.6.10

Every irreducible element in $\mathbb{Z}[i]$ divides some positive prime in \mathbb{Z} . Furthermore, if $zw = p$ for some prime $p \in \mathbb{Z}_{>0}$, then if z, w are non-units then z, w are both irreducible. Even better, if a prime $p \in \mathbb{Z}$ is reducible in $\mathbb{Z}[i]$ if and only if $p = x^2 + y^2, x, y \in \mathbb{Z}$

Proof. If $z = x + yi \in \mathbb{Z}[i]$ is irreducible, then $N(z) = x^2 + y^2 = z\bar{z}$ is an integer greater than 1.

Thus z divides some integer greater than 1. Now simply factor $N(z) = p_1 p_2 \cdots p_k$ as a product of primes within \mathbb{Z} . Then apply the fact that irreducibles are prime in a PID to see that z divides p_j for some j .

For the other direction, if $zw = p$, then $N(z)N(w) = N(p) = p^2$, so $N(z) = N(w) = p$. Great! This means z, w are irreducible. Even better $z = N(z) = z\bar{z}$. Similarly if $p = x^2 + y^2$, we see that $p = (x + yi)(x - yi)$. 

Now to find the irreducibles, we can factor primes in \mathbb{Z} over $\mathbb{Z}[i]$. Trivially we see:

$$2 = (1 + i)(1 - i) = -i(1 + i)^2.$$

Now we know p is reducible if and only if $p = x^2 + y^2$. Reducing mod 4, we see

$$p \equiv (0 \text{ or } 1) + (0 \text{ or } 1).$$

But then p is prime so it can't be two zeros or two ones. Thus $p \equiv_4 1$ provided that p is reducible.

Therefore if $p \equiv_4 3$ (and p is a positive prime in \mathbb{Z}) then p is irreducible in $\mathbb{Z}[i]$.

If we instead reduce mod p we see $0 \equiv_p x^2 + y^2$. Thus $x^2 = -y^2$. We see y cannot be divisible by p from $p = x^2 + y^2$. Thus $(xy^{-1})^2 \equiv_p -1$.

Therefore, -1 is a square in $(\mathbb{Z}/p\mathbb{Z})^\times$. Now we show the converse.


If $a^2 \equiv_p -1$ for some $a \in \mathbb{Z}$, we will show somehow that $p = x^2 + y^2$. Why? Well, $p \mid (a^2 + 1)$ in \mathbb{Z} , so $p \mid (a + i)(a - i)$ in $\mathbb{Z}[i]$. We know $p \nmid a \pm i$, so p is not prime in $\mathbb{Z}[i]$, so it is not irreducible.

Thus we have the following result for $p > 0$ a prime in \mathbb{Z}

$$p \text{ reducible in } \mathbb{Z}[i] \iff p = x^2 + y^2, x, y \in \mathbb{Z} \iff -1 \equiv a^2 \pmod{p}, a \in \mathbb{Z}.$$

Know: If $p = 2$ then -1 is a square mod p , and if $p \equiv_4 3$ then -1 is not a square mod p .


Show: If $p \equiv_4 1$ then -1 is a square mod p .

Proof 1. We claim that $((p-1)/2)!$ is $-1 \pmod{p}$. 

Proof 2. $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order divisible by 4, thus it has an order 4-element a , then a^2 has order 2, implying $a^2 \equiv_p -1$.

Note: to show $x^2 \equiv_p 1$ implies $x \equiv_p \pm 1$ we see $p \mid x^2 - 1 = (x-1)(x+1)$, so $p \mid x-1$ or $p \mid x+1$. 

Proof 3. Consider the squaring map $(\mathbb{Z}/p\mathbb{Z})^\times \rightarrow (\mathbb{Z}/p\mathbb{Z})^\times$. This is a homomorphism with kernel ± 1 . Thus the image has size $(p-1)/2$, which is even.

Therefore by Cauchy's theorem, the image has an order 2 element by Cauchy's theorem. But the only such element is -1 , so -1 is a square mod p . 

Lemma II.6.11


If K is a field, $f(x) \in K[x]$ has degree $d > 0$, then $f(x)$ has at most d roots.

Proof. $c \in K$ implies $f(x) = (x-c)g(x) + r$ for $r \in K$. Evaluate at $x = c$, then $f(c) = r$. If $f(c) = 0$, $x-c \mid f(x)$ in $K[x]$.

But $x-c$ is irreducible in $K[x]$, thus $x-c$ is one of the irreducibles showing up in the unique prime factorization of $f(x)$.

Clearly $c \neq c'$ implies $x-c, x-c'$ are not unit multiples of one another. We can factor f in $K[x]$ as a constant $u \in K^\times$ times polynomials

$$u \cdot (x-c_1)(x-c_2) \cdots (x-c_\ell) \cdot (\text{product of irreducibles with degree} \geq 2).$$

for $c_i \in K$. Then $d = \ell + \text{sum of degrees of large irreducibles}$. Thus $d \geq \ell \geq \# \text{ roots}$. 

Corollary II.6.12

If R is an integral domain, then any nonzero $f \in R[x]$ has $\leq \deg(f)$ roots in $\text{Frac}(R)$, and hence $\leq \deg(f)$ roots in R .

But this fails in non-integral domains.

Example II.6.4

Note $2x$ has roots $0, 2$ in $\mathbb{Z}/4\mathbb{Z}$. And $x^2 - 1$ has roots $\pm 1, \pm 3$ in $\mathbb{Z}/8\mathbb{Z}$.

Lemma II.6.13

If $p > 2$ is prime in \mathbb{Z} and $a \in \mathbb{Z}$ with $p \nmid a$, then x is a square mod p if and only if $a^{\frac{p-1}{2}} \equiv_p 1$.


Proof. The polynomial $x^{\frac{p-1}{2}} - 1$ has $\leq (p-1)/2$ roots in $\mathbb{Z}/p\mathbb{Z}$. But if $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ then


$$(a^2)^{\frac{p-1}{2}} = a^{p-1} \equiv 1 \pmod{p}.$$

Therefore all the squares are roots of this equation (using Lagrange's Theorem).

Now we just count the squares. We claim that $1^2, 2^2, \dots, ((p-1)/2)^2$ are distinct mod p (the rest are negatives of these, so have the same squares).

Since if $x^2 \equiv_p y^2$, then $p \mid (x-y)(x+y)$. Therefore $x = y$ or $x = -y$. This doesn't happen for the above when $0 < x < y < p/2$.

Thus by counting, the roots of $x^{\frac{p-1}{2}} - 1$ are precisely the squares modulo p . 

Proof 4. If $p \equiv_4 1$, then $(-1)^{(p-1)/2} = 1$, which implies -1 is a square. 

Of course not all domains are UFDs, such as

Example II.6.5

$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ in $\mathbb{Z}[\sqrt{-5}]$. Then $2, 3, 1 \pm \sqrt{-5}$ are all irreducible and not unit multiples of one another.

This implies $\mathbb{Z}[\sqrt{-5}]$ is NOT a UFD.

Factorign in $\mathbb{Z}[x]$ versus in $\mathbb{Q}[x]$.

$\mathbb{Z}[x]$		$\mathbb{Q}[x]$
± 1	units	\mathbb{Q}^\times

If $p \in \mathbb{Z}$ is prime, then p is irreducible in $\mathbb{Z}[x]$, but p is a unit in $\mathbb{Q}[x]$.

Given nonzero $f(x) \in \mathbb{Z}[x]$, let $c := \gcd(\text{coeffs of } f)$ (called the “content” of f) then write $f(x) = c \cdot \hat{f}(x)$

Where $\hat{f}(x) \in \mathbb{Z}[x]$ has content 1. We say $\hat{f}(x)$ is “primitive.”

Note: A nonzero $f(x) \in \mathbb{Z}[x]$ is primitive if and only if the image of $f(x)$ in $(\mathbb{Z}/p\mathbb{Z})[x]$ is nonzero for all prime p .

Consequence: If $g, h \in \mathbb{Z}[x]$ are primitive, then gh is primitive, since if p is prime and \bar{g}, \bar{h} are the image of g, h in $(\mathbb{Z}/p\mathbb{Z})[x]$, then $\bar{g}\bar{h} \neq 0$.

Proposition II.6.14

If $f(x) \in \mathbb{Z}[x]$ is primitive and irreducible (in $\mathbb{Z}[x]$), then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Proof. If $f(x) = g(x)h(x)$ for $g, h \in \mathbb{Q}[x]$ non-constant. Then $g = \frac{a}{b}\hat{g}(x)$ where $a, b \in \mathbb{Z} \setminus \{0\}$ are coprime and $\hat{g}(x) \in \mathbb{Z}[x]$ is primitive.

Likewise write $h = \frac{c}{d}\hat{h}(x)$ with the same conditions. Then

$$bdf(x) = ac\hat{g}(x)\hat{h}(x).$$

But then $\hat{g}(x)\hat{h}(x)$ is primitive.

Finish next time! 

Let R be a UFD, $K := \text{Frac}(R)$.

Note that in a UFD, gcd makes sense (at least in terms of divisors up to units, not in terms of Bezout). Namely, to get $\gcd(a, b)$, factor a, b into irreducibles, and then take as many powers of common irreducibles as possible.

Theorem II.6.15

$R[x]$ is a UFD.

Note this implies that $R[x_1, \dots, x_n]$ is a UFD.

Proof. First note that $(K[x])^\times = K^\times \supseteq R^\times = (R[x])^\times$.

For any nonconstant $f(x) := \sum_{i=0}^n a_i x^i$ in $R[x]$, define the “content” of $f(x)$ to be

$$\text{cont}(f) := \gcd(a_0, a_1, \dots, a_n).$$

Thus $f(x) = \text{cont}(f)\hat{f}(x)$ where $\hat{f}(x) \in R[x] \setminus R$ and $\text{cont}(\hat{f}) = 1$ (equivalently a unit).

If $f(x) \in R[x] \setminus R$ has $\text{cont}(f) = 1$, say $f(x)$ is “primitive.” Note that if $f(x) \in R[x] \setminus R$ is irreducible, then $\text{cont}(f) = 1$ by the above factorization.

So: The irreducibles in $R[x]$ are

- Irreducible elements in R (those are units in $K[x]$)
- Nonconstant irreducibles in $R[x]$ (these are primitive).

We’ll show that the irreducible polynomials in $K[x]$ are precisely the primitive irreducible polynomials in $R[x]$ times elements of K^\times .

Any nonconstant $f(x) \in K[x]$ can be written as $\frac{a}{b}\hat{f}(x)$ with $\hat{f}(x) \in R[x]$ primitive and $a, b \in R \setminus \{0\}$. We may assume that $\gcd(a, b) = 1$.

If $f, g \in R[x]$ are primitive then fg is primitive. We prove the contrapositive. Suppose that $\text{cont}(fg) \neq 1$, then there is some irreducible $p \in R$ such that $p \mid \text{cont}(fg)$. We can then consider the homomorphism $\phi : R[x] \rightarrow (R/(p))[x]$. Then $\phi(fg) = 0$, meaning $\phi(f)\phi(g) = 0$. But then p is irreducible, R is a UFD, so p is prime, then $R/(p)$ is an integral domain, and so is $(R/(p))[x]$. Thus $\phi(f)$ or $\phi(g) = 0$. Then p divides the coefficients of one of these, so $p \mid \text{cont}(f)$ or $p \mid \text{cont}(g)$. Thus f or g is not primitive. f or g is not primitive.

Claim

If $f \in R[x]$ is irreducible and primitive, then f is irreducible in $K[x]$

Suppose $f = gh$ for $g, h \in K[x]$ nonconstant. We may assume that $g \in R[x]$ is primitive by moving the “ a/b portion” and absorbing it into h .


Then $h(x) = \frac{a}{b}\hat{h}(x)$ where $\hat{h}(x) \in R[x]$ is primitive and a, b are coprime. Then $bf = ag\hat{h}$, with f, g, \hat{h} all primitive. Then $g\hat{h}$ is primitive as well. We see $b \mid a$ and $a \mid b$ because of primitiveness. Thus $a = bu$ for a unit $u \in R^\times$, so $f = ug\hat{h}$. But wait! $ug, \hat{h} \in R[x]$ are not constants!

This is impossible since f is irreducible in $R[x]$!

Now if $f, g \in R[x]$ are primitive then $f \in gR^\times$ if and only if $f \in gK^\times$. The first direction is clear, for the other direction, if $f = \frac{a}{b}g$ for $a, b \in R \setminus \{0\}$ coprime. Then $bf = ag$, by primitiveness $a \mid b, b \mid a$, so we can cancel to get $f = ug$ for some unit $u \in R^\times$ where $a = bu$.

Now given any $f(x) \in R[x]$ which is not zero, if $f(x) \in R$ then the unique factorization from R is the unique factorization in $R[x]$. If $\deg f > 0$, then $f = \text{cont}(f)\hat{f}(x)$ for primitive \hat{f} . So there is a factorization of $f(x)$ in $R[x]$ by appending factorizations of $\text{cont}(f) \in R$ and of $\hat{f}(x)$ (for example by going to $K[x]$ and using primitiveness).

Conversely, any factorization of $f(x)$ in $R[x]$ must consist of a unit times irreducibles with product $\text{cont}(f)$ times irreducibles with product \hat{f} , again using primitiveness. The factorization of $\text{cont}(f)$ is unique since R is a UFD, and higher degree polynomials cannot multiply to become constants. The factorization of $\hat{f}(x)$ consists of primitives, and is then the unique factorization in $K[x]$. But because of the above this is not a concern (as uniqueness is the same in both settings).

Thus $R[x]$ is a UFD. 


Proposition II.6.16 (Eisensteins Irreducibility Criterion)

If $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 \in \mathbb{Z}[x]$ and for some prime p , we have that $p \nmid a_n$, $p \mid a_{n-1}, \dots, a_0$, $p^2 \nmid a_0$, and $\text{cont}(f) = 1$ (e.g. when $a_n = 1$), then $f(x)$ is irreducible in $\mathbb{Z}[x]$ (and hence in $\mathbb{Q}[x]$).

Proof. Let $\phi : \mathbb{Z}[x] \rightarrow (\mathbb{Z}/p\mathbb{Z})[x]$. We know that $\phi(f) = a_n x^n \neq 0$. If $f = gh$ with $g, h \in \mathbb{Z}[x]$ nonconstant then $\phi(f) = \phi(g)\phi(h)$. Because $p \nmid a_n$ we see that

$$\deg(\phi(g)) = \deg(g) \qquad \deg(\phi(h)) = \deg(h).$$

Then $\phi(g) = bx^i$, $\phi(h) = dx^{n-i}$ for $b, d \in (\mathbb{Z}/p\mathbb{Z})^\times$ and $0 < i < n$.

Then we have that $p \mid g(0), p \mid h(0)$, so $p^2 \mid g(0)h(0) = a_0$, and this is a contradiction. 

Corollary II.6.17

$x^n - p$ is irreducible in $\mathbb{Q}[x]$ for all $n > 0$ and every prime p .

Next time: Deduce that $x^{p-1} + \dots + 1$ is irreducible in $\mathbb{Q}[x]$ for all primes p .

Corollary II.6.18

For prime p , $\Phi_p(x) = x^{p-1} + \dots + 1$ is irreducible in $\mathbb{Q}[x]$.

Proof. Note that $\Phi_p(x) = \frac{x^p - 1}{x - 1}$. Thus

$$\begin{aligned} \Phi_p(x+1) &= \frac{(x+1)^p - 1}{x} \\ &= x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \dots + \binom{p}{p-1}. \end{aligned}$$

Note then that $\binom{p}{p-1} = p$, and $p \mid \binom{p}{i}$ for $1 \leq i < p-1$.

Then $\Phi_p(x+1)$ is irreducible in $\mathbb{Q}[x]$ by Eisenstein. Thus $\Phi_p(x)$ is irreducible in $\mathbb{Q}[x]$. 

Just so you've seen it because it's awesome.

Theorem II.6.19 (Frobenius's Density Theorem)

For $f(x) \in \mathbb{Q}[x]$ of degree n , and any partition P of n . Then

$$\lim_{N \rightarrow \infty} \frac{\# \text{ primes } p \leq N \text{ s.t. } P = \text{degrees of irr. factors of } f \text{ in } \mathbb{F}_p[x]}{\# \text{ primes } \leq N}$$

is equal to

$$\frac{\#\{g \in G \mid P = \text{cycle lengths of } g\}}{\#G}$$

where G is the Galois group of $f(x)$ over \mathbb{Q} (which we'll define later as a subgroup of S_n).

Consequences:

- (1) $f(x)$ factors into degree 1 polynomials in $\mathbb{F}_p(x)$ for at least $\frac{1}{n!}$ of all primes p . But in fact it is exactly $\frac{1}{\#G}$ where G is the galois group.
- (2) If $f(x) \in \mathbb{Q}[x]$ of degree n , then $f(x)$ has a root mod p for at least $1/n$ of all primes p .

This is because at least $1/n$ elements of any subgroup of S_n have a fixed point.

Analogous Result: If $f(x) \in \mathbb{F}_p[x]$ has degree n , and $\#f(\mathbb{F}_p) < p$, then $\#f(\mathbb{F}_p) \leq p - (p-1)/n$.

Definition II.6.4 (Prime Ideals)

An ideal $P \neq (1)$ of a ring R is prime if $ab \in P$ implies that $a \in P$ or $b \in P$ for all $a, b \in R$.

(so if $P = (p)$ with $p \in R$, then P is a prime ideal if and only if p is a prime element).

Note: P is a prime ideal if and only if R/P is an integral domain. So: all maximal ideals are prime.

Recall II.6.6

If I, J are ideals of R , then

$$IJ = \left\{ \sum_{k=1}^n i_k j_k \mid i_k \in I, j_k \in J \right\}$$

Example II.6.7

Recall that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD since $2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Further all these are irreducible except 6, and the units are exactly ± 1 , so no two of these are unit multiples.

We see that

$$(2, 1 + \sqrt{-5}) = (2, 1 - \sqrt{-5})$$

$$(3, 1 + \sqrt{-5}) = (3, 1 - \sqrt{-5})$$

are prime ideals. But in $\mathbb{Z}[\sqrt{-5}]$, every ideal except (0) , (1) is a product of prime ideals in exactly one way (up to permuting the prime ideals).

Then in $\mathbb{Z}[\sqrt{-5}]$:

$$(2, 1 + \sqrt{-5})^2 = (4, 2 + 2\sqrt{-5}, -4 + 2\sqrt{-5}) = (2)$$

$$(6) = (2)(3) = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

$$(2, 3) = (2, 1 + \sqrt{-5})^2(3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5})$$

$$(1 + \sqrt{-5})(1 - \sqrt{-5}) = (2, 1 + \sqrt{-5})(3, 1 + \sqrt{-5})(2, 1 - \sqrt{-5})(3, 1 - \sqrt{-5}).$$

This factorization is in fact unique.

Example II.6.8

In contrast, $\mathbb{Z}[2i]$ does NOT have unique prime factorization of ideals.

$$(-4) = (2i)(2i) = (2)(-2).$$

Definition II.6.5 (Dedekind Domain)

A Dedekind Domain is an integral domain with unique prime factorization of ideals. These will not be used in this course.

Fact: If $K = \mathbb{Q}[x]/(f(x))$ where $f(x) \in \mathbb{Q}[x]$ is irreducible, and R is the ring of all algebraic integers in K (i.e. roots of monic polynomials in $\mathbb{Z}[x]$), then R is a Dedekind Domain.

For example, $\mathbb{Z}[\sqrt{d}]$ is a Dedekind domain if $d \in \mathbb{Z} \setminus \{0, 1\}$ is square-free and $d \not\equiv 1 \pmod{4}$.

Example II.6.9

$\mathbb{Z}[x]$ is a UFD.

$\mathbb{Z}[x]/(x^2 + 5) \cong \mathbb{Z}[\sqrt{-5}]$ is not a UFD.

More generally: R is a UFD implies $R[x]$ is a UFD, but R/I need not be a UFD (even when I is a prime ideal).

Likewise, R is a PID does not imply $R[x]$ is a PID (e.g. $\mathbb{Z}[x]$ is not a PID), but R/I is a PID for all prime ideals I .

Even better, R is Noetherian implies $R[x]$ is Noetherian (Hilbert basis theorem), and R/I is Noetherian for any ideal I .

Lemma II.6.20

Let R be a UFD and $K = \text{Frac}(R)$. If $\alpha \in K$ is a root of a monic polynomial in $R[x]$, then $\alpha \in R$.

Proof. Say α is a root of $x^n + a_1x^{n-1} + \cdots + a_n$ with $a_i \in R$. Write $\alpha = u/v$ where $u, v \in R$ are coprime.

Then we see that

$$\frac{u^n}{v^n} + a_1 \frac{u^{n-1}}{v^{n-1}} + \cdots + a_{n-1} \frac{u}{v} + a_n = 0.$$

Multiplying by v^n we see

$$u^n + a_1 u^{n-1} v + a_2 u^{n-2} v^2 + \cdots + a_{n-1} u v^{n-1} + a_n v^n.$$

If v were not a unit, it would have some irreducible/prime factor p , but then $p \mid u^n$ because it divides all the other terms. But then $p \mid u$, and this is a contradiction since u, v are coprime.

Therefore v is a unit and $\alpha \in R$.



III. Midterm Review

Midterm: Monday 6PM-8:30PM.

If R is a UFD, say a nonconstant $f(x) \in R[x]$ is “primitive” if $\gcd(\text{coeffs of } f) = 1$.

Any nonconstant $f(x) \in R[x]$ can be written as a constant $c \in R$ times a nonconstant primitive polynomial $\hat{f}(x) \in R[x]$

Then any nonconstant irreducible $f(x) \in R[x]$ is primitive. And if $K := \text{Frac}(R)$, then f remains irreducible in $K[x]$.

Any nonconstant $f(x) \in K[x]$ can be written as $c \cdot \hat{f}(x)$, $c \in K^\times$, $\hat{f}(x) \in R[x]$ primitive. Then $f(x)$ is irreducible in $K[x]$ if and only if $\hat{f}(x)$ is irreducible in $R[x]$.

All nonzero constants in K are units in K , but there can be nonzero constants which are nonunits in $R[x]$.

- Ideals (see Definition II.2.7): Kernels of ring homomorphisms, aka non-empty subsets of R which are preserved under (finite) R -linear combinations.
 - If I is an ideal of R , then there is a quotient map $R \rightarrow R/I$ which is a surjective ring homomorphism.

Conversely, if $R \rightarrow S$ is a surjective ring homomorphism, then there exists an isomorphism $R/I \rightarrow S$ such that

$$\begin{array}{ccc} R & \xrightarrow{\quad} & S \\ & \searrow & \nearrow \\ & R/I & \end{array}$$

commutes.

- Correspondence Theorem (see Theorem II.2.9) If $R \xrightarrow{\varphi} S$ is a surjective ring homomorphism. Then the maps

$$\begin{aligned} I &\mapsto \varphi(I) \\ \varphi^{-1}(J) &\leftarrow J \end{aligned}$$

are inverse bijections

$$\{\text{ideals of } R \text{ containing } \ker \varphi\} \xleftrightarrow{\quad} \{\text{ideals of } S\}$$

Also if $I \supseteq \ker \varphi$ then $R/I \cong S/\varphi(I)$. See Example II.2.7 for a great example of a use case for this. Namely proving that $\mathbb{Z}[i]/(2+i) \cong \mathbb{Z}/5\mathbb{Z}$.

- Basics of Polynomial Rings
 - Evaluation Maps (see Definition II.3.3). If $\varphi : R \rightarrow S$ is a homomorphism, and $s \in S$ is a fixed element, then there is a unique extension of φ to $\hat{\varphi} : R[x] \rightarrow S$ taking x to s .
Note if $\varphi : R \rightarrow S$ this gives a unique extension $\hat{\varphi} : R[x] \rightarrow S[x]$ which sends x to x . We can do the same thing in many variables.
 - Polynomial Division (see Theorem II.3.1): If $f(x), g(x) \in R[x]$ and $g(x) \neq 0$ is monic, then there exists a unique $q(x), r(x) \in R[x]$ such that

$$f(x) = g(x)q(x) + r(x)$$

and $\deg r < \deg g$.

- Quotient by a monic (see Example II.4.3). If $f(x) \in R[x]$ is monic and nonconstant, then $R \hookrightarrow R[x] \rightarrow R[x]/(f(x))$ is injective. Even better, each element of $R[x]/(f(x))$ can be written in exactly one way as $a(x) + (f(x))$ with $\deg(a) < \deg f$ by long division.
In contrast, if $R = \mathbb{Z}/(4)$ then $R[x]/(2x-1) = 0$ does not have this property.

- Field of Fractions (see Theorem II.4.2): Every integral domain has a field of fractions K .
Even better if L is a field containing R , then $L \supseteq K \supseteq R$ with $K \cong \text{Frac}(R)$.
This is called the “resultant” of $ax^2 + bx + c, 2ax + b$.
- Maximal Ideals (see Definition II.5.1): An ideal M of R is maximal (that is $M \neq R$ and $M \subsetneq I$ for an ideal I implies $I = R$). This holds if and only if R/M is a field.
 - Hilbert’s Nullstellensatz (Theorem II.5.5) The maximal ideals of $\mathbb{C}[x_1, \dots, x_n]$ are $(x_1 - \alpha_1, \dots, x_n - \alpha_n)$ with $\alpha_1, \dots, \alpha_n \in \mathbb{C}$.
- Euclidean Rings, PIDs, UFDs (see Section II.6)
 - R is Euclidean $\implies R$ is a PID $\implies R$ is a UFD. $\mathbb{Z}[x], \mathbb{C}[x, y]$ shows the second converse doesn’t hold and $\mathbb{Z}[\alpha]$ for $\alpha = (1 + \sqrt{-19})/2$ shows the first converse doesn’t hold.
This comes in a few parts. PIDs are clearly Noetherian, and Proposition II.6.6 gives that all PIDs have a factorization, and Proposition II.4.1 gives uniqueness.
Then Lemma II.6.7 gives that Euclidean \implies PID.
 - If R is a UFD and $p \in R$ is irreducible then p is prime.
 - If R is an integral domain and $p \in R$ is prime, then p is irreducible (see Lemma II.6.1).
 - Non-UFD’s $\mathbb{Z}[\sqrt{-5}]$.
- Useful ideas
 - The norm function $\mathbb{C}^\times \rightarrow \mathbb{C}^\times$ given by $a + bi \mapsto a^2 + b^2 = (a + bi)(a - bi)$ is very useful.
Restrict to $\mathbb{Z}[i], \mathbb{Z}[\sqrt{-2}], \dots$, then the images are in \mathbb{Z} and we can use these to show Euclidean-ness. Even for the counterexample of $\alpha = (1 + \sqrt{-19})/2$ we can use this to show $\mathbb{Z}[\alpha]$ is a PID.
 - For other algebraic integers, for example $\mathbb{Z}[\sqrt{2}]$ we can take $a + b\sqrt{2} \mapsto |(a + b\sqrt{2})(a - b\sqrt{2})| = |a^2 - 2b^2|$.
This is then a multiplicative function $\mathbb{Z}[\sqrt{2}] \rightarrow \mathbb{Z}$. We will work with generalizations later.
- Good to recall Bezout’s Theorem (see Theorem II.5.11).

What can you say when two polynomials $f, g \in R[x]$ have a common root in some ring containing R .

Example III.0.1

Consider $ax^2 + bx + c$ and its derivative $2ax + b$. Then, pretending R is an integral domain (really working over $\mathbb{Z}[A, B, C, x]$ and then going to $R[x]$ by a nice map) we have

$$ax^2 + bx + c = (2ax + b) \left(\frac{x}{2} + \frac{b}{4a} \right) + \left(c - \frac{b^2}{4a} \right).$$

Then we have that

$$\begin{aligned} 4a(ax^2 + bx + c) &= (2ax + b)(2ax + b) + (4ac - b^2) \\ 4a^2x^2 + 4abx + 4ac &= (2ax + b)(2ax + b) + (4ac - b^2). \end{aligned}$$

Any common zero of these in a ring containing R would be a zero of $4ac - b^2$. Thus $4ac - b^2 = 0$.

Alternately: If A, B, C are independent variables over \mathbb{Q} , then

(1) Do Euclid's algorithm in $(\mathbb{Q}[A, B, C])[x]$ on $AX^2, BX + C, 2Ax + B$ to get

$$1 = (Ax^2 + Bx + C) \cdot u(x) + (2Ax + B) \cdot v(x)$$

for $u, v \in (\mathbb{Q}(A, B, C))[x]$ and then let $\Delta(x) \in \mathbb{Z}[A, B, C][x]$ be a common denominator of u, v .

Then multiply. Then $\Delta = \mathbb{Z}[A, B, C]$ is some linear combination of $Ax^2 + Bx + C, 2Ax + B$.

Then apply $\mathbb{Z}[A, B, C][x] \rightarrow R[x]$, given by mapping $A \mapsto a, B \mapsto b, C \mapsto c, x \mapsto x$. Conclude that the image of Δ is a $R[x]$ -linear combination of $ax^2 + bx + c, 2ax + b$.

This is called the “resultant” of $ax^2 + bx + c, 2ax + b$.

IV. Galois Theory

IV.1. Field Extensions

Definition IV.1.1

Given a field K , a field L containing K is called an extension of K and L/K (**NOT A QUOTIENT!**) is a field extension

Definition IV.1.2

If L/K is a field extension, then its degree is $\dim_K L$, that is the dimension of L as a K -vector space.

Notation: We often denote the degree by $[L : K] = \dim_K L$.

Definition IV.1.3

Let L/K be a field extension and let $\alpha \in L$. Then $K(\alpha)$ is the smallest field containing K and α , that is

$$K(\alpha) := \left\{ \frac{a(\alpha)}{b(\alpha)} : a, b \in K[X], b(\alpha) \neq 0 \right\}.$$

Let $S = \{f(x) \in K[x] : f(\alpha) = 0\}$. Then S is an ideal of $K[x]$ (closed under linear combinations). Therefore $S = (m(x))$ for some $m(x) \in K[x]$ because $K[x]$ is principal. Furthermore, if $S \neq 0$ then $m(x)$ is a nonzero polynomial of minimal degree in S , because we can use the division algorithm in a field.

Even better, we may assume $m(x)$ is monic or zero, by multiplying by units, and clearly $m(x)$ is irreducible because if $m(x) = f(x)g(x)$, $f(\alpha), g(\alpha) = 0$ because we're in an integral domain, and then $m \mid f$ or $m \mid g$.

Great!

Definition IV.1.4

α is called algebraic over K if $f(\alpha) = 0$ for some nonzero $f(x) \in K[x]$. In this case, the minimal polynomial of α over K is

$$\text{minpol}_K(\alpha) = \text{irr}_K(\alpha)$$

is the unique monic irreducible polynomial in $K[x]$ such that $\text{irr}_K(\alpha) = 0$.

α is called transcendental over K if α is not algebraic over K .

If α is transcendental then $K[x] \hookrightarrow K[\alpha] \subseteq K(\alpha)$ by evaluation, and being transcendental implies injectivity. This then gives an isomorphism of rings $K[x] \cong K[\alpha]$, and it extends to an isomorphism $K(x) \cong K(\alpha)$ as well.

This means intuitively that we can treat a transcendental α as a formal variable x .

Now suppose $\alpha \in L$ is algebraic over K , with $m(x) = \text{irr}_K(\alpha)$. Then $K[x] \rightarrow K[\alpha]$ is a surjection, with kernel $(m(x))$. Then

$$K[x]/(m(x)) \cong K[\alpha]$$

and because $(m(x))$ is a maximal ideal since m is irreducible, we know that $K[\alpha]$ is a field, and $K[\alpha] = K(\alpha)$.

We see that $K[\alpha] \cong K[x]/(m(x))$ is a K -vector space with basis $1, x, \dots, x^{n-1}$ where $n := \deg(m)$ by the polynomial division algorithm, as each coset in $K[x]/(m(x))$ has a unique representative of degree $< n$.

Perfect! This implies that

Proposition IV.1.1

If α is algebraic over K , and $n := \deg(\text{irr}_K(\alpha))$, then $K[\alpha] = K(\alpha)$ has basis $1, \alpha, \dots, \alpha^{n-1}$ as a K -vector space, and so

$$\dim_K K(\alpha) = n = \deg(\text{irr}_K(\alpha)).$$

Example IV.1.1

We have that for p a prime,

$$[\mathbb{Q}(i) : \mathbb{Q}] = 2$$

$$[\mathbb{Q}(\sqrt[p]{p}) : \mathbb{Q}] = n$$

$$[\mathbb{Q}(e^{2\pi i/p}) : \mathbb{Q}] = p - 1.$$

The second follows from Eisenstein because $x^n - p$ is irreducible, and this actually extends to $p \neq 1$ and not a square. The second follows because $\text{irr}_{\mathbb{Q}}(e^{2\pi i/p}) = x^{p-1} + x^{p-2} + \dots + 1$. We showed this was irreducible using Eisenstein as well.

Note that if you have a polynomial with α as a root, it gives an upper bound on the degree of $[K(\alpha) : K]$.

Example IV.1.2

Any n -dimensional \mathbb{C} -vector space has dimension $2n$ as an \mathbb{R} -vector space. If $\alpha_1, \dots, \alpha_n$ is a \mathbb{C} -basis, then every element of the vector space can be written in exactly one way as

$$\sum (a_j + ib_j)\alpha_j$$

so $\alpha_1, i\alpha_1, \dots, \alpha_n, i\alpha_n$ is an \mathbb{R} -basis.

Proposition IV.1.2

If L/K is a field extension and V is an L -vector space, then

$$\dim_K V = [L : K] \cdot \dim_L(V).$$

Proof. Let $\alpha_1, \alpha_2, \dots, \alpha_n$ be an L -basis for V and let $\beta_1, \beta_2, \dots, \beta_m$ be a K -basis for L . We show $\{\beta_i \alpha_j\}$ is a K -basis for V .

Every element of V can be written in exactly one way as $\sum_j \ell_j \alpha_j$ with $\ell_j \in L$. Each ℓ_j can be written in exactly one way as $\sum_i k_{ij} \beta_i$ with $k_{ij} \in K$.

Therefore every element of V can be written in exactly one way as $\sum_j \sum_i k_{ij} \beta_i \alpha_j$. This shows $\{\beta_i \alpha_j\}$ is a K -basis for V .

Note: It is nice to know this basis.



Corollary IV.1.3

if K, L, M are fields with $M \supseteq L \supseteq K$ then

$$[M : K] = [M : L] \cdot [L : K].$$

Example IV.1.3

By Eisensteins, $x^n - p$ is irreducible over \mathbb{Q} for any prime p . Thus

$$[\mathbb{Q}(\sqrt[n]{p}) : \mathbb{Q}] = n.$$

Therefore if K is a field containing $\sqrt[n]{p}$, then $[K : \mathbb{Q}]$ is divisible by n or is infinite.

Note also that if $\alpha \in K$ has a square root in L , then $[K(\sqrt{\alpha}) : K] = 1$ or 2 since there is a degree 2 polynomial with $\sqrt{\alpha}$ as a root.

Then if $\alpha_1 \in \mathbb{Q}$, define $K_1 = \mathbb{Q}(\sqrt{\alpha_1})$, and inductively let $\alpha_{i+1} \in K_i$, $K_{i+1} = \mathbb{Q}(\sqrt{\alpha_1}, \dots, \sqrt{\alpha_{i+1}})$. Then

$$[K_{i+1} : K_i] = 1 \text{ or } 2.$$

Thus $[K_i : \mathbb{Q}]$ divides 2^i .

If n is not a power of 2, then $n \nmid [K_i : \mathbb{Q}]$. Therefore $\sqrt[n]{p} \notin K_i$. Wait! This shows things such as

$$\sqrt[3]{2} \neq \sqrt{1 + \sqrt{1 + \sqrt{2}}} - \sqrt{\frac{1}{2} + \sqrt{3}}$$

as the latter is contained in such a field K_i , namely take $\alpha_1 = 2, \alpha_2 = 3, \alpha_3 = 1 + \sqrt{2}, \alpha_4 = 1/2 + \sqrt{3}, \alpha_5 = 1 + \sqrt{\alpha_3}$.

Thus, $\sqrt[n]{p}$ cannot be expressed as successive sums, multiplications, divisions, or square roots of elements of \mathbb{Q} when p is a prime and n is not a power of 2. This can be extended to when p is not a perfect square fairly easily.

Specifically, $\sqrt[3]{2}$ cannot be expressed this way.

IV.2. Motivation: Constructions with Straight Edge and Compass

This section will not be tested, and we will return to fields after the break.

You start with two points. We will call these A, B , and we will think of the distance between them as being one.

Build from these: points, lines, circles. Here are the rules:

- Given 2 points, you can construct the line passing through them.
- Given 2 points, you can construct the circle centered at one point and passing through the other.
- Given 2 lines (or 2 circles or 1 line, 1 circle), then you can construct the points on their intersection.

Definition IV.2.1

A number $\ell \in \mathbb{R}$ is constructible if, with straight edge and compass, we can construct a point C on the line through A, B such that the signed distance from A to C is ℓ times the signed distance from A to B .


Theorem IV.2.1

A number $\ell \in \mathbb{R}$ is constructible if and only if $\ell \in K_n$ where $\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n$ where $K_i = K_{i-1}(\sqrt{\alpha_i})$ with $\alpha_i \in K_{i-1} \cap \mathbb{R}_{>0}$.

Corollary IV.2.2

If $\ell \in \mathbb{R}$ is constructible then $[\mathbb{Q}(\ell) : \mathbb{Q}] = 2^m$ for some $m \in \mathbb{Z}_{\geq 0}$.

The converse is badly false, most numbers whose degree is a power of two are not constructible.

Proof. We see $[K_n : \mathbb{Q}]$ is a power of two, and $[K_n : \mathbb{Q}] = [K_n : \mathbb{Q}(\ell)][\mathbb{Q}(\ell) : \mathbb{Q}]$, so $[\mathbb{Q}(\ell) : \mathbb{Q}]$ is a power of two. 

First, we'll look at the consequences

- (1) Impossible to “duplicate a cube,” i.e., construct a cube whose volume is twice that of a given cube. That is $\sqrt[3]{2}$ is not constructible, which we did last time, since $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.
- (2) Impossible to “square the circle,” i.e., construct a square whose area is that of a given circle. I.e., $\sqrt{\pi}$ is not constructible, true because $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}] = \infty$.
- (3) Impossible to “trisect an arbitrary angle,” since $\cos 60^\circ = 1/2$ is constructible, but $\cos 20^\circ$ is not. We know this because

$$\cos(3\theta) = 4 \cos^3 \theta - 3 \cos \theta$$

$$\frac{1}{2} = 4 \cos^3 20^\circ - 3 \cos 20^\circ$$

Thus $\cos 20^\circ$ is a root of $8x^3 - 3x - 1$. Substituting $y = x/2$ we get

$$y^3 - 3y - 1$$

which is irreducible in $\mathbb{F}_2[y]$, so it is irreducible in $\mathbb{Z}[y]$, so it is irreducible in $\mathbb{Q}[y]$. Perfect! Thus $[\mathbb{Q}(\cos 20^\circ) : \mathbb{Q}] = 3$.

Gauss somehow figured out that

$$\cos \frac{2\pi}{17} = \frac{1}{16} + \frac{\sqrt{17}}{16} + \frac{\sqrt{34-2\sqrt{17}}}{16} + \frac{1}{8} \sqrt{17 + 3\sqrt{17} - \sqrt{34-2\sqrt{17}} - 2\sqrt{34+2\sqrt{17}}}$$

We can then build a tower

$$\begin{array}{c} \mathbb{Q}\left(\sqrt{17},\sqrt{34+2\sqrt{17}},\cos 2\pi/17\right) \\ \quad \downarrow 2 \\ \mathbb{Q}\left(\sqrt{17},\sqrt{34+2\sqrt{17}}\right) \\ \quad \downarrow 2 \\ \mathbb{Q}(\sqrt{17}) \\ \quad \downarrow 2 \\ \mathbb{Q} \end{array}$$

showing that $\cos(2\pi/17)$ is constructible.

Claim

We can construct a regular n -gon if and only if we can construct $\cos(2\pi/n)$.

Corollary IV.2.3

If p is prime and a regular p -gon is constructible, then p must be a Fermat prime, that is $p = 2^k + 1$ (which implies $k = 2^\ell$, $\ell \geq 0$ or $\ell = -\infty$).

Proof. If $\alpha = e^{2\pi i/p}$, then we have that

$$\frac{\alpha + \frac{1}{\alpha}}{2} = \cos \frac{2\pi}{2}$$

$$\alpha^2 - \left(2 \cos \frac{2\pi}{p}\right) \alpha + 1 = 0.$$

Thus we have that

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\cos 2\pi/p, \alpha) : \mathbb{Q}(\cos 2\pi/p)] \leq 2.$$

And because $\alpha \notin \mathbb{R}$, $\cos 2\pi/p \in \mathbb{R}$, that the degree is exactly two.

But $\text{irr}_{\mathbb{Q}}(\alpha) = x^{p-1} + \cdots + 1$. Therefore

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = p - 1.$$

Therefore, we have a tower of extensions

$$\begin{array}{c}
\mathbb{Q}(\alpha) \\
\downarrow 2 \\
\mathbb{Q}(\cos 2\pi/p) \\
\downarrow (p-1)/2 \\
\mathbb{Q}
\end{array}
\quad \begin{array}{l} \\ \\ p-1 \\ \\ \end{array}$$

So we must have that $p - 1 = 2^k$ if the regular p -gon is constructible as desired.



Lemma IV.2.4

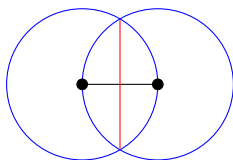
Given two points, can construct the perpendicular bisector of the segment between them.

Given a line ℓ and a point p , can construct a line through p which is perpendicular to ℓ .

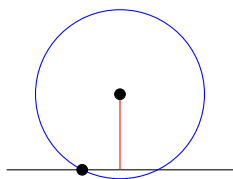
Given a line ℓ and a point p , can construct a line through p and a parallel to ℓ .

Given points p, q, r and a line ℓ containing r , can construct a point s on ℓ such that the segments rs and pq have the same length.

Proof. Let's go! To get perpendicular bisectors, we see that



is a perpendicular bisector. To get perpendiculars, we just see that



We can construct parallels by drawing perpendiculars twice



The last is left as an exercise!



Npte: Given p, q , you can construct a line through p with angle θ from the line pq if and only if $\cos \theta$ is constructible. This is because you can drop perpendiculars.

Proof of Theorem IV.2.1, forward. Let $K \subseteq \mathbb{R}$ be a field which we're working over.

A line through 2 points with coordinates in a field K has an equation over K . Similarly a circle with center a point over K passing through a point over K has an equation over K .

The intersection of two lines with equations over K is either \emptyset or a point with coordinates in K .

The intersection of a line with coordinates in K with a circle with coordinates in K is either \emptyset , a point with coordinates in K , two points with coordinates in K , or two points with coordinates in $K(\alpha)$ for some $\alpha \in K, \alpha > 0$.

Intersecting two circles: We may center one of the circles at 0. Then we have $x^2 + y^2 = r_1, (x-a)^2 + (y-b)^2 = r_2$, where $r_1, r_2, a, b \in K$. Then we see that (x, y) must satisfy

$$-2ax + a^2 - 2by + b^2 = r_2 - r_1$$

If $(a, b) \neq (0, 0)$ then this defines a line over K , and so the intersection of these two circles over K is either the same as the intersection of the first circle with a line over K .

Thus the intersection is either \emptyset , a point over K , two points over K , or two points over $K(\sqrt{\alpha})$ where $\alpha \in K, \alpha > 0$.

This proves the forward direction. If a number $\ell \in \mathbb{R}$ is constructible then it belongs to a tower of field extensions of degrees 1 or 2.



Proof of Theorem IV.2.1, converse. if a, b are constructible, then so are $a + b$, $-a$ (by circles), and ab by drawing perpendiculars and using similar triangles.

Similarly we can construct $1/a$ with similar triangles.

We can also construct \sqrt{a} , also by similar triangles and circles.



IV.3. More Field Extensions / Splitting Fields

Recall IV.3.1

The characteristic of a ring R is the order of 1_R under addition if this order is finite, and 0 if this order is not finite. Put another way it is the unique positive generator of the kernel of the map $\varphi : \mathbb{Z} \rightarrow R$.

If R is an integral domain (more specifically when R is a field), $\text{char } R$ must be 0 or a prime, because

$$\frac{\mathbb{Z}}{\ker \varphi} \cong \text{im } \varphi \subseteq R.$$

And so $\text{im } \varphi$ is an integral domain, so $\ker \varphi$ is a prime ideal.

Example IV.3.2

$\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}(x)$ all have characteristic 0. Note that if $L \supseteq K$ then $\text{char}(L) = \text{char}(K)$.

Also note that for $n \in \mathbb{Z}$, $\text{char}(R) \mid n$ if and only if $n = 0$ in R .

For K a field, $\text{char}(K) \nmid n$ if and only if $n \in K^\times$.

Definition IV.3.1 (Frobenius Map)

If $p := \text{char}(K)$ is positive, then the map $x \mapsto x^p$ is a homomorphism, called the Frobenius Map.

This holds since $(xy)^p = x^p y^p$, and

$$(x + y)^p = x^p + \binom{p}{1} x^{p-1} y + \cdots + \binom{p}{p-1} x y^{p-1} + y^p = x^p + y^p$$

because if $1 \leq k \leq p-1$ then $\binom{p}{k} = p!/k!(p-k)!$ is divisible by p .

Example IV.3.3

In characteristic two, $(x + y)^2 = x^2 + 2xy + y^2 = x^2 + y^2$.

In characteristic three, $(x + y)^3 = x^3 + 3x^2y + 3xy^2 + y^3 = x^3 + y^3$.

Note: A homomorphism $K \rightarrow L$ of fields is injective, because the kernel is an ideal of K , and so is either (0) or (1). But $1 \mapsto 1$, so 1 does not lie in the kernel. Thus the kernel is (0).

Recall IV.3.4

If K is a field, $\alpha \in L$, $L \supseteq K$, then α is algebraic over K provided that α is a root of a nonzero polynomial in $K[x]$.

Then the kernel of $K[x] \xrightarrow{\text{ev}_\alpha} K$ is a prime ideal, and so it is generated by a unique monic irreducible polynomial with α as a root. We call this the minimal polynomial of α .

If this minimal polynomial has degree n , then $1, \alpha, \dots, \alpha^{n-1}$ is a basis of $K[\alpha]$ as a K -vector space and


$$K[\alpha] = K(\alpha) = \frac{K[x]}{(\text{minimal polynomial of } \alpha)}$$

$$[K(\alpha) : K] = \deg(\text{minimal polynomial of } \alpha).$$

Then note that L/K has degree 1 if and only if $L = K$.

Proposition IV.3.1

If L/K has degree p for p a prime, and $L \supseteq M \supseteq K$. Then $M = L = K$.

Proof. We see that $[L : K] = [L : M][M : K]$, so one of $[L : M]$ or $[M : K]$ is one. 

Proposition IV.3.2

Suppose K is a field and $\text{char}(K) \neq 2$. Then L/K has degree two if and only if $L = K[\sqrt{d}]$ for some $d \in K$ with no $e \in K$ such that $e^2 = d$.

\Leftarrow is clear by the minimal polynomial $x^2 - d$.


Proof. Let $\alpha \in L, \alpha \notin K$. By Proposition IV.3.1 we have that $L = K(\alpha)$. Now let $f(x)$ be the minimal polynomial of f . Then $\deg f = 2, f$ is monic, so $f(x) = x^2 - bx - a$ for some $a, b \in K$.

Then $\alpha^2 - b\alpha = a$. If $\text{char}(K) \neq 2$ then

$$\left(\alpha - \frac{b}{2}\right)^2 = a + \frac{b^2}{4}.$$

Then $\alpha - b/2 \notin K, -\alpha + b/2 \notin K$ are distinct. Thus

$$L = K(\alpha - b/2) = K[\sqrt{a + b^2/4}].$$

If L/K has degree 2, $\text{char}(K) = 2$, $\alpha \in L \setminus K$, then $\alpha^2 + b\alpha = a$ for some $a, b \in K$. If $b \neq 0$ then 

$$\frac{\alpha^2}{b^2} + \frac{\alpha}{b} = \frac{a}{b^2}$$

so α/b is a root of $x^2 + x = a/b^2$, $L = K(\alpha/b)$. If $b = 0$, then α is a root of $x^2 = a$, then $L = K(\alpha)$ and $x^2 - a = (x - \alpha)^2$.

Remark IV.3.1

We will throw away adjoining p -th roots in characteristic p because they behave badly (in the future see the definitions of separable/inseparable, Definition IV.4.3).

Example IV.3.5

If $L = \mathbb{Q}(\sqrt[3]{2}), K = \mathbb{Q}$ then $L = \mathbb{Q}(\sqrt[3]{4} + 5\sqrt[3]{2} + 1)$ by Proposition IV.3.1.

More generally the minimal polynomial of $a\sqrt[3]{4} + b\sqrt[3]{2} + c$ over \mathbb{Q} has degree three for all $a, b, c \in \mathbb{Q}$ with a, b not both 0. Thus we've learned something about infinitely many polynomials by only knowing about $x^3 - 2$.

Note: if K is a field, $f \in K[X]$ is irreducible, then $L := K[X]/(f(X))$ is a field, and if α is the image of x in L then $f(\alpha) = 0$ and $L = K[\alpha] = K(\alpha)$.

Definition IV.3.2


For $g(x) \in K[x] \setminus K$, a splitting field of $g(x)$ over K is a field $L \supseteq K$ such that $g(x)$ factors into linears in $L[x]$ as $c \cdot (x - \alpha_1) \cdots (x - \alpha_n)$ for $c \in K, \alpha_i \in L$, and $L = K(\alpha_1, \dots, \alpha_n)$.

Proposition IV.3.3

Splitting Fields exist

Proof. Given $g(x) \in K[x] \setminus K$, we may assume g is monic by multiplying by a unit in K .

If g factors into linears over K , then K is itself the splitting field. Otherwise, let g_1 be an irreducible factor of $g(x)$ in $K[x]$ of degree greater than 1, and let $K_1 = K[x]/(g_1(x))$.

Now g has more irreducible factors in $K_1[x]$ than $K[x]$. g has at most $\deg g$ irreducible factors in any $L[x]$, $L \supseteq K$. So repeat until you get K_1, K_2, \dots, K_n as the splitting field of g over K . 

Our next goal is to prove the uniqueness of splitting fields. That is given $g(x) \in K[x] \setminus K$ and L, L' are splitting fields over K , then there is an isomorphism $L \rightarrow L'$ which is the identity on K .

Amazing Fact: If L is a splitting field of $g(x)$ over K and $h(x) \in K[x]$ is irreducible and has a root in L , then $h(x)$ factors into linears in $L[x]$, so L contains a splitting field of $h(x)$ over K .

Recall IV.3.6

If L is a field containing K , and $\alpha \in L$, then $K(\alpha)$ is the smallest subfield of L containing K and α .

Explicitly, it's $\{a(\alpha)/b(\alpha) \mid a, b \in K[X], b(\alpha) \neq 0\}$. If α is algebraic over K , then

$$K(\alpha) = K[\alpha] \cong K[X]/(f(X))$$

where $f = \text{minpoly}_K(\alpha)$.

Last time: For any field K , and any irreducible $f(X) \in K[X]$, there exists a field L containing K such that $f(x)$ has a root in L , namely $K[Y]/(f(Y))$.

Example IV.3.7

Consider $x^3 - 2$ over \mathbb{Q} . It's irreducible by Eisenstein, and it has a root in $\mathbb{Q}[Y]/(Y^3 - 2)$, namely $\bar{Y} = Y + (Y^3 - 2)\mathbb{Q}[Y]$.

In \mathbb{C} , there are three roots of $x^3 - 2$, $\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$ for $\omega = e^{2\pi i/3}$.

So adjoining a cube root of 2 to \mathbb{Q} (in \mathbb{C}) yields $\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\omega\sqrt[3]{2}), \mathbb{Q}(\omega^2\sqrt[3]{2})$.

Furthermore, each of these is isomorphic to $\mathbb{Q}[Y]/(Y^3 - 2)$. In other words

$$\text{Hom}_{\mathbb{Q}}(\mathbb{Q}[Y]/(Y^3 - 2), \mathbb{C}) \text{ has size 3.}$$

These are given by $\bar{Y} \mapsto \sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$.

Proposition IV.3.4

If L is a field containing K , and $\alpha \in L$ has minimal polynomial $f(X)$ over K , then

$$\text{Hom}_K(K[X]/(f(X)), L) \cong \text{Hom}_K(K(\alpha), L)$$

is in bijection with $\{\text{roots of } f(X) \text{ in } L\}$.

That is the number of roots of $\text{minpoly}_K(\alpha)$ in L only depends on the isomorphism class of $K(\alpha)$ over K .

Proof. Note $K(\alpha) = K[\alpha]$. Now if $\sigma \in \text{Hom}_K(K(\alpha), L)$, then $\beta := \sigma(\alpha)$ has

$$f(\beta) = f(\sigma(\alpha)) = \sigma(f(\alpha)) = \sigma(0) = 0$$


because σ is the identity on K (can do this explicitly but why). Furthermore, σ is determined by $\sigma(\alpha)$ because $K(\alpha) = K[\alpha]$.

Conversely, if $\beta \in L$ is a root of $f(X)$, then we know

$$\begin{aligned} K(\beta) &\cong_K \frac{K[Y]}{(f(Y))} \cong_K K(\alpha) \\ \beta &\mapsto \bar{Y} \mapsto \alpha. \end{aligned}$$

So there is a map

$$\begin{aligned} K[\alpha] &\cong_K K[\beta] \\ \alpha &\mapsto \beta. \end{aligned}$$

Thus the inclusion $K(\alpha) \cong_K K[\beta] \hookrightarrow L$ gives us a map in $\text{Hom}_K(K(\alpha), L)$ mapping α to β . 

Corollary IV.3.5

Suppose $\varphi : K \rightarrow L$ is a homomorphism between fields, M/K is a field extension, and $\alpha \in M$ is algebraic over K with minimal polynomial $f(X)$.

Then the # of extensions of φ to a homomorphism $K(\alpha) \rightarrow L$ equals the number of roots of $f^\varphi(X) \in L[X]$, where $f^\varphi(X)$ is the image of $f(X)$ under the extension $\varphi : K[X] \rightarrow L[X]$.


Proof. Let $K' := \varphi(K)$, then $\varphi : K \cong K'$. Therefore

$$\text{Hom}_{K'}(K'[Z]/(f^\varphi(Z)), L) \cong \{\# \text{ of roots of } f^\varphi \text{ in } L\}.$$

Now we need to show that elements $\text{Hom}_{K'}(K'[Z]/(f^\varphi(Z)), L)$ are exactly extensions of φ to $K(\alpha) \rightarrow L$.

Well, under $\varphi : K \rightarrow K'$ we have the isomorphism

$$K(\alpha) \cong K[Y]/(f(Y)) \cong K'[Z]/(f^\varphi(Z))$$

Composition of a map $\text{Hom}_{K'}(K'[Z]/(f^\varphi(Z)), L)$ with this isomorphism is exactly an extension of φ . 

Proposition IV.3.6

Suppose L, M are splitting fields of $f(x) \in K[x] \setminus K$ over K .

Then there is an isomorphism $L \rightarrow M$ which is the identity on K .

Uniqueness of Splitting Fields. Given $f(X) \in K[X] \setminus K$, let L and M be splitting fields of $f(X)$ over K .

Let $f_1(x) \in K[X]$ be an irreducible factor of $f(X)$ having degree at least two (if no such factor exists then $L = K = M$). Let $\alpha_1 \in L$ be a root of $f_1(X)$.

Then $\text{Hom}_K(K(\alpha_1), M)$ is the number of roots of $f_1(X)$ in M by Proposition IV.3.4. Then there are that many choices for $\varphi_1 : K(\alpha_1) \cong K(\beta_1) \subseteq M$ as below

$$\begin{array}{ccc} L & & M \\ & \searrow^{\varphi_1} & \\ K(\alpha_1) & \xrightarrow{\quad} & K(\beta_1) \\ | & & | \\ K & \xrightarrow{\text{Id}} & K \end{array}$$

Call $L_1 = K(\alpha_1)$, $M_1 = K(\beta_1)$. If $f(X)$ factors into linears over $L_1[X]$ then $f(X) = f^{\varphi_1}(X)$ factors into linears in $M_1[X]$. Then $L_1 = L$, $M_1 = M$, $\varphi_1 : L_1 \xrightarrow{\cong} M_1$.


Otherwise, let $f_2(X) \in L_1[X]$ be an irreducible factor of $f(X)$ with degree at least two. Let $\alpha_2 \in L$ be a root of $f_2(X)$. Then by Corollary IV.3.5 the number of extensions of φ_1 to a homomorphism $L_1(\alpha_2) \rightarrow M$ is the number of roots of $f_2^{\varphi_1}(X)$ in M , which is positive.

Thus there are that many choices for $\varphi_2 : L_1(\alpha_2) \cong M_1(\beta_2) \subseteq M$ as

$$\begin{array}{ccc} L & & M \\ & & \\ L_1(\alpha_2) & \xrightarrow{\varphi_2} & M_1(\beta_2) \\ | & & | \\ K(\alpha_1) & \xrightarrow{\varphi_1} & K(\beta_1) \\ | & & | \\ K & \xrightarrow{\text{Id}} & K \end{array}$$

Because $L_1(\alpha_2) = K(\alpha_1, \alpha_2)$ this ends up with the following picture

$$\begin{array}{ccc} L & & M \\ & & \\ K(\alpha_1, \alpha_2, \alpha_3) & \xrightarrow{\varphi_3} & K(\beta_1, \beta_2, \beta_3) \\ | & & | \\ K(\alpha_1, \alpha_2) & \xrightarrow{\varphi_2} & K(\beta_1, \beta_2) \\ | & & | \\ K(\alpha_1) & \xrightarrow{\varphi_1} & K(\beta_1) \\ | & & | \\ K & \xrightarrow{\text{Id}} & K \end{array}$$

We claim this process eventually terminates. Why? Well f has at most $\deg f$ roots in L , and at each step we select a root $\alpha_i \in L$ of a degree two irr. factor of f in $L_{i-1}[X]$ (where $x - \alpha_j$ are now factors for $j < i$). Thus $\alpha_i \neq \alpha_1, \dots, \alpha_{i-1}$. 

Even better: The number of choices of φ_1 is exactly

$$\# \text{ roots of } f_1(X) \text{ in } M \leq \deg(f_1) = [K(\alpha_1) : K] \leq \deg(f)$$

(the \leq is almost always equal). Likewise, after choosing φ_1 , the $\#$ of choices for φ_2 is

$$\# \text{ of roots of } f_2^{\varphi_1}(x) \text{ in } M \leq \deg(f_2) = [K(\alpha_1, \alpha_2) : K(\alpha_1)] \leq \deg(f) - 1.$$

Corollary IV.3.7

Let L, M be splitting fields of f over K , then

$$\# \text{Hom}_K(L, M) \leq [L : K] \leq \deg(f)!$$

First inequality is almost always equal. We can then choose $L = M$, and then $\text{Hom}_K(L, M) = \text{Aut}_K(L)$.

Last time: Given a field K , and a nonconstant $f(X) \in K[X]$, there exists a splitting field of $f(X)$ over K . Furthermore, if L, M are both splitting fields of $f(X)$ over K then there is a K -isomorphism (fixing K) $L \rightarrow M$.

We also showed that if N is a splitting field of $f(X)$ over K , then $|\text{Aut}_K(N)| \leq [N : K]$, and I claim that usually this is equality.

$$\begin{array}{ccc}
 N & \xrightarrow{\varphi} & N \\
 & & \\
 K(\alpha_1, \alpha_2, \alpha_3) & \xrightarrow{\varphi_3} & K(\beta_1, \beta_2, \beta_3) \\
 | & & | \\
 K(\alpha_1, \alpha_2) & \xrightarrow{\varphi_2} & K(\beta_1, \beta_2) \\
 | & & | \\
 K(\alpha_1) & \xrightarrow{\varphi_1} & K(\beta_1) \\
 | & & | \\
 K & \xrightarrow{\text{Id}} & K
 \end{array}$$

where α_i is a root of an irreducible factor $f_i(X)$ of $f(X)$ in $K(\alpha_1, \dots, \alpha_{i-1})[X]$. The number of choices for φ_1 is the number of roots of $f_1(X)$ in N which is $\leq \deg(f_1) = [K(\alpha_1) : K]$. We just continue here.

The number of choices for φ_i given a choice for $\varphi_1, \dots, \varphi_{i-1}$ is the number of roots β_i of $f_i^{\varphi_{i-1}}(X)$ which is

$$\leq \deg(f_i) = [K(\alpha_1, \dots, \alpha_i) : K(\alpha_1, \dots, \alpha_{i-1})]$$

If we have equality that

$$\# \text{ of roots of } f_i^{\varphi_{i-1}}(X) \text{ in } N \stackrel{?}{=} \deg(f_i) = [K(\alpha_1, \dots, \alpha_i) : K(\alpha_1, \dots, \alpha_{i-1})]$$

then we'll have the desired equality. Conclude that

$$|\text{Aut}_K(N)| \leq [K(\alpha_1) : K] \cdot [K(\alpha_1, \alpha_2) : K(\alpha_1)] \cdots = [N : K].$$

Proposition IV.3.8

If L/K is a finite extension and M/K is any extension, then

$$|\text{Hom}_K(L, M)| \leq [L : K]$$

Proof. DIY, same proof.



Example IV.3.8

Consider $x^3 - 1$ over \mathbb{Q} . Well, this factors as $(x - 1)(x^2 + x + 1)$.

Then we look at

$$\frac{\mathbb{Q}[X]}{(x^2 + x + 1)} \cong \mathbb{Q}(e^{2\pi i/3}).$$

This is the splitting field, as

$$x^3 - 1 = (x - 1)(x - e^{2\pi i/3})p(x)$$

and $\deg p = 1$, so it has a root. Particularly if $\omega := e^{2\pi i/3}$.

Then

$$\begin{aligned}
 (x^3 - 1) &= (x - 1)(x - \omega)(x - \omega^2) \\
 \text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\omega)) &= \{\text{Id}, z \mapsto \bar{z}\}
 \end{aligned}$$

$$= \{\omega \mapsto \omega, \omega \mapsto \bar{\omega} = \omega^2 = -\omega - w\}.$$

Example IV.3.9

The splitting field of $x^3 - 2$ over \mathbb{Q} . The roots are $\alpha, \alpha\omega, \alpha\omega^2$ where $\alpha := \sqrt[3]{2}$. Building our tower

$$\mathbb{Q}(\alpha, \omega) \xrightarrow{\varphi_2} \mathbb{Q}(\beta, \hat{\omega})$$

$$\mathbb{Q}(\alpha) \xrightarrow{\varphi_1} \mathbb{Q}(\beta)$$

$$\mathbb{Q} \xrightarrow{\text{Id}} \mathbb{Q}$$

where $\beta = \alpha, \alpha\omega, \alpha\omega^2$, and $\hat{\omega} = \omega, \omega^2$.

Then $\text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha, \omega)) \cong S_3$, since it is a subgroup of S_3 (determined by how it permutes the roots), and it has six things in it.

IV.4. Separability**Definition IV.4.1** (Separable)

A nonzero $f(X) \in K[X]$ is separable if it has $\deg(f)$ distinct roots in a splitting field of f/K .

Definition IV.4.2

A field K is perfect if all irreducible polynomials over K are separable.

We'll show: all fields of characteristic 0 are perfect and finite fields are perfect.

Note: $f(X)$ is separable if and only if $f(X)$ is the product of coprime separable irreducible polynomials.

Lemma IV.4.1

If an irreducible $f(X) \in K[X]$ is NOT separable then $p := \text{char}(K)$ is positive and $f(x) = g(x^p)$ for some $g \in K[X]$.

Proof. If f is non-separable, and L is the splitting field of f/K then there is an $\alpha \in L, h(x) \in L[x]$ with

$$(x - \alpha)^2 h(x) = f(x)$$

$$2(x - \alpha)h(x) + (x - \alpha)^2 h'(x) = f'(x)$$

$$0 = f'(\alpha).$$

But $f(x)$ is irreducible and $f(\alpha) = 0$, so $f = \text{minpoly}_K(\alpha)$. So since $f'(\alpha) = 0$ and $\deg(f') < \deg(f)$, we know that $f'(x) = 0$.

This never happens in characteristic zero, because then $f'(x) = 0$ if and only if f is constant. Thus $p := \text{char}(K) > 0$. We then see that

$$f(X) = \sum_{i=0}^n a_i X^i$$

$$f(X) = \sum_{i=1}^n i a_i X^{i-1}.$$

Thus $ia_i = 0$. If $i = 0$, then $p \mid i$. Thus we can write f as

$$f(X) = \sum_{j=0}^n a_{pj} X^{pj} = g(X^p).$$

Where $a_{pj} = 0$ if $pj > n$.



Corollary IV.4.2

If $\text{char}(K) = 0$ then K is perfect.

Corollary IV.4.3

If $\text{char}(K) = 0$ and N/K is the splitting field over K of some $f(X) \in K[X]$ then

$$|\text{Aut}_K(N)| = [N : K].$$

Definition IV.4.3

Given an extension L/K , then $\alpha \in L$ is separable over K provided that α is algebraic over K and $\text{minpoly}_K(\alpha)$ is separable.

L/K is separable provided that every $\alpha \in L$ is separable over K .

L/K is algebraic if every $\alpha \in L$ is algebraic over K .

Note: If α is algebraic over K , then α is separable over K if and only if

$$|\text{Hom}_K(K(\alpha), N)| = [K(\alpha) : K]$$

for some extension N/K (say the algebraic closure of N or a splitting field of the minimal polynomial of α).

Lemma IV.4.4

If L/K is finite then L/K is separable if and only if $|\text{Hom}_K(L, N)| = [L : K]$ for some N/K

Proof. $L = K(\alpha_1, \dots, \alpha_n)$ for some $\alpha_1, \dots, \alpha_n \in L$ (which we can pick at will).

We form a tower as before

$$\begin{array}{ccc} L & \xrightarrow{\varphi} & N \\ K(\alpha_1, \alpha_2, \alpha_3) & \xrightarrow{\varphi_3} & \\ \downarrow & & \\ K(\alpha_1, \alpha_2) & \xrightarrow{\varphi_2} & \\ \downarrow & & \\ K(\alpha_1) & \xrightarrow{\varphi_1} & \\ \downarrow & & \\ K & \xrightarrow{\text{Id}} & K \end{array}$$


where the # of choices for φ_i given φ_{i-1} is

$$\leq [K(\alpha_1, \dots, \alpha_i) : K(\alpha_1, \dots, \alpha_{i-1})]$$

with equality if and only if α_i is separable over K . Then

$$\begin{aligned} |\mathrm{Hom}_K(L, N)| &\leq [K(\alpha_1) : K][K(\alpha_1, \alpha_2) : K(\alpha_1)] \cdots \\ &= [L : K] \end{aligned}$$

The equality is true when L/K is separable.

For the converse, choose α_1 to be any element of L . The # of choices for φ_1 has to agree with $[K(\alpha_1) : K]$ if and only if α_1 is separable over K , and this has to agree if we are to have the desired equality. 


Corollary IV.4.5

If M/L and L/K are finite, then M/K is separable if and only if M/L is separable and L/K is separable.

The \implies is clear.

Proof. If L/K and M/L are separable then there exists N/K such that

$$|\mathrm{Hom}_K(L, N)| = [L : K] \qquad |\mathrm{Hom}_L(M, N)| = [M : L]$$

So there exist $[L : K]$ K -homomorphisms $L \rightarrow N$ and each of these can be extended in $[M : L]$ ways to a homomorphism $M \rightarrow N$ yielding $[M : K]$ K -homomorphisms $M \rightarrow N$. 

Recall IV.4.1

A finite extension L/K is separable if and only if $|\mathrm{Hom}_K(L, \Omega)| = [L : K]$ for some extension Ω/K (think of \mathbb{C} for \mathbb{Q} or the algebraic closure of K).

We used this to prove: If M/L and L/K are finite extensions then M/K is separable if and only if both M/L and L/K are separable.

Also: If $\mathrm{char} = 0$ then all algebraic extensions of K are separable (K is called perfect).

Corollary IV.4.6

If $\alpha_1, \dots, \alpha_n$ are separable over K then $K(\alpha_1, \dots, \alpha_n)/K$ is separable.

Corollary IV.4.7

If $f(X) \in K[X]$ is separable and N is a splitting field of $f(X)$ over K then

$$|\mathrm{Aut}_K(N)| = [N : K]$$

IV.5. Finite Fields

If K is a finite field, then $p := \mathrm{char}$ is a positive prime and K contains \mathbb{F}_p (the additive group generated by 1 in K). Thus K is an \mathbb{F}_p -vector space of dimension n (since it's finite).

Thus $|K| = p^n$. Our plan is to show there is exactly one such field for every choice of p, n .

Proposition IV.5.1

There is exactly one finite field K of size $q = p^n$ for a prime p and $n \geq 1$ up to isomorphism.

Notation: We write \mathbb{F}_q for “the” finite field of size q .

Proof. If K is a finite field, say of size q , then K^\times has order $q - 1$. Lagrange's theorem tells us that for $\alpha \in K^\times$ gives $\alpha^{q-1} = 1$. Therefore every $\alpha \in K$ satisfies $\alpha^q = \alpha$.


This shows that every $\alpha \in K$ is a root of $x^q - x$. Thus K is a splitting field of $x^q - x$ over \mathbb{F}_p . Any two splitting fields are isomorphic, so this is clear.

Conversely, if $q = p^n$, then let S be the set of roots of $x^q - x$ in a splitting field of $x^q - x$ over \mathbb{F}_p .

- (1) $|S| = q$ since $(x^q - x)' = -1$ has no roots, so there are no repeated roots.
- (2) S is closed under multiplication and addition.

Note that the map $\alpha \mapsto \alpha^p$ is the Frobenius homomorphism (Definition IV.3.1), and $\alpha \mapsto \alpha^q$ is the composition of this map with itself so it is a field homomorphism. Thus if α, β are roots of $x^q - x$ then

$$\begin{aligned}(\alpha\beta)^q &= \alpha^q \beta^q = \alpha\beta \\ (\alpha + \beta)^q &= \alpha^q + \beta^q = \alpha + \beta.\end{aligned}$$

Finite nonempty sets which are closed under addition and multiplication are fields (inverses come for free). Thus S is a field of size q . 

Remark IV.5.1

Note that \mathbb{F}_8 does not contain \mathbb{F}_4 because 8 is not a power of 4.

Proposition IV.5.2

$\mathbb{F}_q \supseteq \mathbb{F}_r$ if and only if they have the same characteristic p and $q = r^k$ for some k .

This means that $r = p^\ell$, so $q = p^{\ell k}$.


Proof. The forward direction holds because field extensions always have the same characteristic, and \mathbb{F}_q is a finite vector space over \mathbb{F}_r , and so it has some dimension k .

Conversely, if $\ell \mid n$ then $\mathbb{F}_{p^n} \supseteq \mathbb{F}_{p^\ell}$ since \mathbb{F}_{p^n} is the roots of $x^{p^n} - x$ and $x^{p^\ell} - x$ divides $x^{p^n} - x$.

Lets use that the Frobenius map (and its compositions) are an isomorphism. Then

$$\begin{aligned}& x^{p^\ell} - x + (x^{p^\ell} - x)^{p^\ell} + (x^{p^\ell} - x)^{p^{2\ell}} + \cdots + (x^{p^\ell} - x)^{p^{(k-1)\ell}} \\& (x^{p^\ell} - x) + (x^{p^{2\ell}} - x^{p^\ell}) + (x^{p^{3\ell}} - x^{p^{2\ell}}) + \cdots + (x^{p^n} - x^{p^{(k-1)\ell}}) \\& = x^{p^n} - x\end{aligned}$$

Therefore $x^{p^\ell} - x$ divides $x^{p^n} - x$. Then \mathbb{F}_{p^n} is the splitting field of $x^{p^n} - x$ over \mathbb{F}_p . Thus it contains a unique splitting field of the factor $x^{p^\ell} - x$ over \mathbb{F}_p .

Thus $\mathbb{F}_{p^n} \supseteq \mathbb{F}_{p^\ell}$. 

Now we're going to look at the automorphisms of \mathbb{F}_{p^n} . We know we have

$$\text{Frob}_p : x \mapsto x^p$$

is an automorphism. Then we can define

$$\text{Frob}_{p^2} = \text{Frob}_p \circ \text{Frob}_p$$

$$\text{Frob}_{p^k} : x \mapsto x^{p^k}.$$

Note that since \mathbb{F}_{p^n} is the splitting field of $x^{p^n} - x$ we have that $\text{Frob}_{p^n} = \text{Id}$. These are all automorphisms.

They are distinct because for $0 \leq \ell < k < n$, if we have $x^{p^k} = x^{p^\ell}$ for all $x \in \mathbb{F}_{p^n}$ then all p^n elements would be roots of

$$x^{p^k} - x^{p^\ell}$$

which has degree $< p^n$, which is a contradiction.

Then we have that

$$\langle \text{Frob}_p \rangle \subseteq \text{Aut}(\mathbb{F}_{p^n})$$

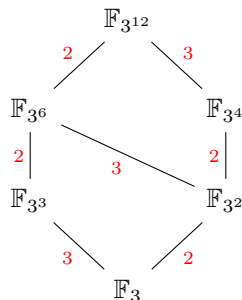
and the LHS has order n , but in general since any automorphism of \mathbb{F}_{p^n} fixes \mathbb{F}_p we have that

$$\text{Aut}(\mathbb{F}_{p^n}) = \text{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^n}) \leq [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$$

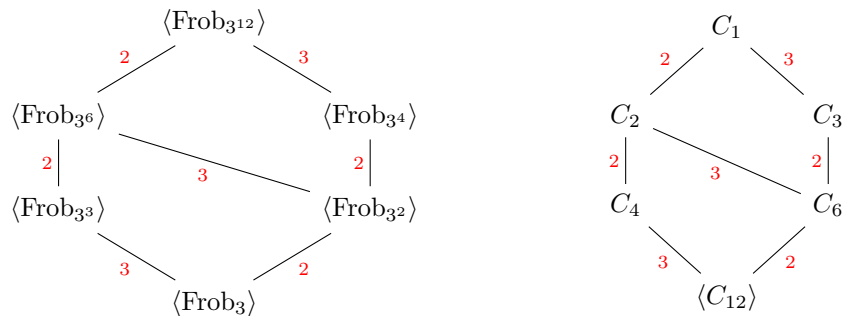
Thus

$$\langle \text{Frob}_p \rangle = \text{Aut}(\mathbb{F}_{p^n}) = \text{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^n})$$

Lets now look at the intermediate fields of $\mathbb{F}_{3^{12}}$. Then we have only the below containments



Now if we look at the subgroups of $\text{Aut}(\mathbb{F}_{3^{12}})$ fixing each intermediate field we get the following corresponding picture, on the right being the abstract cyclic group picture



Note: If L/K is an extension of finite fields and $f(x) \in K[x]$ is minpoly $_K(x)$ for some $\alpha \in L$ then $f(x)$ has $\deg(f)$ distinct roots in L .

Also: if $f(x) \in \mathbb{F}_q[x]$ is irreducible and $\alpha \in \mathbb{F}_{q^n}$ is a root of $f(x)$ then

$$f(x) = (x - \alpha)(x - \alpha^q) \cdots (x - \alpha^{q^{d-1}})$$

where $d = \deg(f)$.

IV.6. Galois Extensions, and the Fundamental Theorem

Definition IV.6.1

A finite extension L/K is Galois if $|\text{Aut}_K(L)| = [L : K]$. In this case we say $\text{Gal}(L/K) := \text{Aut}_K(L)$ is the Galois group of L/K .

Note: We always have $|\text{Aut}_K(L)| \leq [L : K]$. We have shown that a splitting field of a separable polynomial is always a Galois extension.

Definition IV.6.2

Given an extension L/K and some subgroup H of $\text{Aut}_K(L)$ we call $L^H := \{\ell \in L \mid h(\ell) = \ell, \forall h \in H\}$ the fixed field of H .

Theorem IV.6.1 (Fundamental Theorem of Galois Theory)

If L/K is Galois, then there are inverse bijections

$$\{\text{fields } M \text{ with } K \subseteq M \subseteq L\} \leftrightarrow \{\text{subgroups of } G := \text{Gal}(L/K)\}$$

given by

$$M \mapsto \varphi \rightarrow \text{Aut}_M(L)$$

$$L^H \xleftarrow[\psi]{} H$$

where $[L : M] = |\varphi(M)|$, $[M : K] = [G : \varphi(M)]$. Furthermore L/M is Galois with group $\varphi(M)$.

If $K \subseteq M, M' \subseteq L$ then

$$M \supseteq M' \iff \varphi(M) \leq \varphi(M').$$

This gives us the following sort of corresponding picture, if $H := \varphi(M)$, $H' := \varphi(M')$ and $M \supseteq M'$

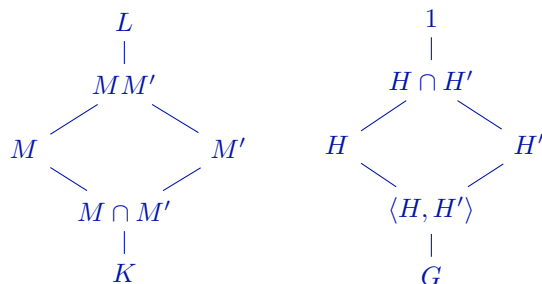
$$\begin{array}{cc} L & 1 \\ | & | \\ M & H \\ | & | \\ M' & H' \\ | & | \\ K & G \end{array}$$

Also

The extension M/K is Galois $\iff \varphi(M)$ is a normal subgroup of G

and in this case $\text{Gal}(M/K) \cong G/\varphi(M)$.

If $K \subseteq M, M' \subseteq L$ then $\varphi(M \cap M') = \langle \varphi(M), \varphi(M') \rangle$ and $\varphi(MM') = \varphi(M) \cap \varphi(M')$. This gives a picture like



For any finite extension K'/K with L, K' living in a common larger field, LK'/K' is Galois, with Galois group isomorphic to $\text{Gal}(L/(L \cap K')) = \varphi(L \cap K')$.

Definition IV.6.3

If $f(X) \in K[X]$ is separable and $n := \deg(f)$, then we know that L/K is Galois where L is the splitting field of $f(X)$ over K .

Note that an element $\sigma \in \text{Gal}(L/K)$ must permute the roots of f , and is determined exactly by how it permutes the roots because $L = K(\text{roots of } f(X))$.

Thus there is an injective homomorphism $\text{Gal}(L/K) \hookrightarrow \{\text{permutations of roots}\} \cong S_n$. Thus we can think of $\text{Gal}(L/K)$ as a subgroup of S_n (at least up to isomorphism).

Define $\text{Gal}(f(X), K) \leq S_n$ to be the image of this homomorphism.

The sizes of the orbits of $\text{Gal}(f(X), K)$ are the degrees of the (monic) irreducible factors of $f(X)$ in $K[X]$.

So: if L is the splitting field of $f(X)$ over K , and K'/K is finite, then

$$\text{Gal}(f(X), K') \cong \text{Gal}(LK'/K') \cong \text{Gal}(L/(L \cap K'))$$

so the degrees of the (monic) irreducible factors of $f(X)$ in $K'[X]$ are the sizes of the orbits of $\text{Gal}(L/(L \cap K')) = \varphi(L \cap K')$.

Thus $f(X)$ is irreducible over K if and only if $\text{Gal}(f(X), K)$ is transitive.

Example IV.6.1

$\text{Gal}((x^2 - 2)(x^2 - 3), \mathbb{Q})$ is not S_4 because we cannot swap $\sqrt{2}$ and $\sqrt{3}$, as $(\sqrt{2})^2 = 2$ but $(\sqrt{3})^2 = 3$. It in fact permutes the roots of $(x^2 - 2)$ and it permutes the roots of $x^2 - 3$.

In fact $\text{Gal}((x^2 - 2)(x^2 - 3), \mathbb{Q}) \cong C_2 \times C_2$ (these are in fact independent).

In contrast, if we have $\text{Gal}((x^2 - 2)(x^2 - 3)(x^2 - 6), \mathbb{Q}) \cong C_2 \times C_2$ because the relation $\sqrt{6} = \sqrt{2}\sqrt{3}$ must be preserved. This can be seen because $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is the splitting field of both polynomials.

Looking at $\text{Gal}(x^4 - 2, \mathbb{Q})$ the only pairs of roots who sum to zero are

$$\begin{aligned} \sqrt[4]{2} + (-\sqrt[4]{2}) &= 0 \\ i\sqrt[4]{2} + (-i\sqrt[4]{2}) &= 0 \end{aligned}$$

Thus we have to preserve or swap the sets $\{\sqrt[4]{2}, -\sqrt[4]{2}\}$ and $\{i\sqrt[4]{2}, -i\sqrt[4]{2}\}$. Magma says that $\text{Gal}(x^4 - 2, \mathbb{Q}) \cong D_4$.

Proof of Theorem IV.6.1, easy/HW bits. We assume the hard parts of the theorem and will prove some of the easier parts.

We know that L/M is Galois because $[L : M] = |\varphi(M)| = |\text{Aut}_M(L)|$.

If $K \subseteq M, M' \subseteq L$, then if $M \supseteq M'$ then any automorphism of L fixing M also fixes M' . Thus

$$\varphi(M) \leq \varphi(M').$$

Likewise if $H \leq H'$, then the elements fixed by H' are also fixed by H , so $L^H \supseteq L^{H'}$.


We will prove on homework that the extension M/K is Galois if and only if $\varphi(M)$ is a normal subgroup of G , and that in this case $\text{Gal}(M/K) \cong G/\varphi(M)$.

Note that $M \cap M'$ is the largest field contained in M, M' , and $\langle \varphi(M), \varphi(M') \rangle$ is the smallest subgroup containing both $\varphi(M), \varphi(M')$. Because φ reverses orders and is a bijection of lattices we have

$$\varphi(M \cap M') = \langle \varphi(M), \varphi(M') \rangle.$$

The other equality follows similarly

$$\varphi(MM') = \varphi(M) \cap \varphi(M').$$

We will prove the statement about a finite extension K'/K on Homework. 

Proof of Theorem IV.6.1, hard parts. First: For any finite L/K and any extension N/K , we have that

$$|\text{Hom}_K(L, N)| \leq [L : K]$$

by sending roots to roots and extending inductively. Also, if L/K is Galois and $N \supseteq L$ then by counting

$$\text{Hom}_K(L, N) = \text{Aut}_K(L).$$

So if L/K is Galois and $K \subseteq M \subseteq L$ we have

$$|\text{Hom}_K(M, L)| \leq [M : L]$$

and each $\varphi \in \text{Hom}_K(M, L)$ can be extended to at most $[L : M]$ elements of $\text{Hom}_K(L, L) \cong \text{Aut}_K(L)$ (by finite-dimensionality and injectivity).

Therefore

$$\begin{aligned} [L : K] &= |\text{Aut}_K(L)| = |\text{Hom}_K(L, L)| \\ &\leq |\text{Hom}_K(M, L)| [L : M] \\ &\leq [M : K][L : M] = [L : K]. \end{aligned}$$

Thus every inequality must be an equality. Thus there are $[M : K]$ elements $\varphi \in \text{Hom}_K(M, L)$ and each of these has $[L : M]$ extensions to $\text{Aut}_K(L)$. Therefore taking $\varphi = \text{Id}_M$ we have

$$|\text{Aut}_M(L)| = |\text{Hom}_M(L, L)| = [L : M].$$

Thus L/M is Galois.

We then know the fixed field

$$L^{\text{Gal}(L/M)} := \{\ell \in L \mid \sigma(\ell) = \ell, \forall \sigma \in \text{Gal}(L/M)\}$$

trivially contains M . We then see that

$$[L : L^{\text{Gal}(L/M)}] \leq [L : M].$$

But then we have

$$[L : L^{\text{Gal}(L/M)}] \geq |\text{Aut}_{L^{\text{Gal}(L/M)}}(L)| = |\text{Gal}(L/M)| = [L : M].$$

Thus $M = L^{\text{Gal}(L/M)}$.

Now we need to show that, conversely, for any subgroup H of $\text{Gal}(L/K)$, that $H = \text{Gal}(L^H)$. We know that

$$\begin{aligned} H &\leq \text{Aut}_{L^H}(L) = \text{Gal}(L/L^H). \\ |H| &\leq [L : L^H]. \end{aligned}$$

But also, L/K is Galois, so it is separable. Thus $L = K(\alpha)$ for some $\alpha \in L$ by the Primitive Element Theorem (see Piazza). Also $L = L^H(\alpha)$.

Call $f := \text{minpoly}_{L^H}(\alpha)$. From the proof of the Theorem B.0.1 (see Appendix), $L^H = K(\text{coeffs of } f)$.

Now consider


$$g(x) := \prod_{\sigma \in H} (X - \sigma(\alpha)).$$

Then

$$\begin{aligned} \sigma(g(x)) &= \prod_{\sigma' \in H} \sigma(X - \sigma'(\alpha)) \\ &= \prod_{\sigma' \in H} (X - \sigma\sigma'(\alpha)) \\ &= g(x). \end{aligned}$$

Thus $g(x) \in L^H[X]$, note that $\deg g = |H|$. Now since $g(\alpha) = 0$ we have $\deg f \leq \deg g$ and may write

$$|H| \leq [L : L^H] = [L^H(\alpha) : L^H] = \deg f \leq \deg g = |H|.$$

Thus $|\text{Gal}(L/L^H)| = [L : L^H] = |H|$, so $H = \text{Gal}(L/L^H)$. 

Example IV.6.2

Say $K = \mathbb{Q}$, L is the splitting field of $x^3 - 2$ over \mathbb{Q} , $\omega = e^{2\pi i/3}$. So $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$. Then $[L : \mathbb{Q}] = 6$. Any $\sigma \in \text{Gal}(L/\mathbb{Q})$ maps $\sqrt[3]{2} \mapsto \sqrt[3]{2}\omega^i$, $i \in \mathbb{Z}/3\mathbb{Z}$ and $\omega \mapsto \omega^j$, $j = 1$ or 2 .

Since the Galois group is size 6, there are at most 6 choices for (i, j) . Thus all choices must work.

Write σ to be the map $\sqrt[3]{2} \mapsto \sqrt[3]{2}\omega$, $\omega \mapsto \omega$ and $\tau : \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega^2$, $\omega \mapsto \omega^2$.


Then $\sigma, \tau \in \text{Gal}(L/\mathbb{Q})$, $\sigma^3 = 1 = \tau^2$, and

$$\tau\sigma\tau^{-1} = \tau\sigma\tau = (\sqrt[3]{2} \mapsto \sqrt[3]{2}\omega^2, \omega \mapsto \omega) = \sigma^2$$

Thus $\text{Gal}(L/\mathbb{Q}) = \langle \tau, \sigma \rangle \cong S_3$.

We may then draw the following complementary lattices

55

Thus $f(x) \in L^G[X] = K[X]$. So since $f(\alpha) = 0$ and all roots of $f(x)$ are in L , all roots of $\text{minpoly}_K(\alpha)$ are in L . 

Proposition IV.6.3 (Natural Irrationalities)

If N/K is Galois, then for any extension L/K (such that N, L are contained in a common field, say M) then the extension NL/L is Galois, and

$$\begin{aligned} \text{Gal}(NL/L) &\cong \text{Gal}(N/(N \cap L)) \\ \sigma &\mapsto \sigma|_N. \end{aligned}$$

Proof. N/K is Galois, so N is the splitting field over K of some separable $f(X) \in K[X]$. Then NL is the splitting field over L of $f(X)$. Thus NL/L is Galois.


For $\sigma \in \text{Gal}(NL/L)$, $\sigma|_N \in \text{Gal}(N/(N \cap L))$ because $\sigma|_{N \cap L} = \text{Id}$, and $\sigma|_N$ is determined by where it sends the roots of $f(X)$, which are permuted by σ , so $\sigma(N) = N$.

φ is injective. If $\sigma \in \ker(\varphi)$, then $\sigma|_N = \text{Id}$, $\sigma \in \text{Gal}(NL/L)$, so $\sigma|_L = \text{Id}$. So then $\sigma = \text{Id}$.

We now show that φ is surjective. Let $H := \text{Gal}(NL/L)$, $G = \text{Gal}(N/(N \cap L))$. We know that $\varphi(H) \leq G$, and $N^{\varphi(H)} \supseteq N \cap L$.

By the Galois Correspondence


$$\begin{aligned} (NL)^H &= L \\ N^{\varphi(H)} &= N \cap L = N^G. \end{aligned}$$

Thus $H = G$, so we're done! 

Lemma IV.6.4

If N/K is Galois and L_1, L_2 are fields containing N , then for any $\sigma \in \text{Hom}_K(L_1, L_2)$, the restriction $\sigma|_N$ lies in $\text{Gal}(N/K)$.

Proof. By Theorem B.0.1 let $N = K(\alpha)$, $f(X)$ be the minimal polynomial of α over K . Then $f(X)$ splits over N .


Then for any $\sigma \in \text{Hom}_K(L_1, L_2)$, $\sigma(\alpha)$ is a root of $f(X)$, so $\sigma(N) = N$. This shows $\sigma|_N$ lies in $\text{Gal}(N/K)$. 

Proposition IV.6.5

If N_1/K and N_2/K are Galois, then N_1N_2/K is Galois, and the map

$$\begin{aligned} \psi : \text{Gal}(N_1N_2/K) &\rightarrow \text{Gal}(N_1/K) \times \text{Gal}(N_2/K) \\ \sigma &\mapsto (\sigma|_{N_1}, \sigma|_{N_2}) \end{aligned}$$

is an injective homomorphism.

Proof. $\sigma|_{N_i} \in \text{Gal}(N_i/K)$, so ψ is well-defined, by a similar argument as the above. Similarly ψ is injective, if $\psi \in \ker(\varphi)$, it is trivial on N_1, N_2 , so it is trivial on N_1N_2 . 

Definition IV.6.4

Say a Galois extension N/K is abelian provided that $\text{Gal}(N/K)$ is abelian.

Corollary IV.6.6

By Proposition IV.6.5, if $N_1/K, \dots, N_\ell/K$ are abelian, then $N_1 N_2 \cdots N_\ell / K$ is abelian.


Corollary IV.6.7

By Proposition IV.6.5, if $N_1/K, \dots, N_\ell/K$ are all Galois with $[N_i : K] = p^{n_i}$, then $[N_1 \cdots N_\ell : K] = p^m$.

Proposition IV.6.8

If N/K and M/K are Galois, then $(N \cap M)/K$ is Galois.

Proof. Any $\sigma \in \text{Hom}_K(N \cap M, NM)$ lifts to an element of $\text{Gal}(NM/K)$, which restricts to automorphisms of N and of M .

Thus $\sigma \in \text{Aut}_K(N_1 \cap N_2)$ from the lemma above. From the fundamental theorem $|\text{Hom}_K(N \cap M, NM)| = [N \cap M : K]$, and so we have $[N \cap M : K]$ things in $\text{Aut}_K(N_1 \cap N_2)$, proving this is Galois. 

Definition IV.6.5

If N/K is Galois and $K \subseteq L \subseteq N$, then the Galois closure of L/K (inside N) is the smallest field M with $L \subseteq M \subseteq N$, and M/K is Galois.

Alternately, if $L = K(\alpha)$, then the Galois closure of L/K is the splitting field of the minimal polynomial of α over K .

Suppose N/K is Galois, $G := \text{Gal}(N/K)$ and $K \subseteq L \subseteq N$, with $H := \text{Gal}(N/L)$. Let N' be the Galois closure of L/K , with $H' := \text{Gal}(N/N')$. We have the pictures

$$\begin{array}{ccc} N & & 1 \\ | & & | \\ N' & & H' \\ | & & | \\ L & & H \\ | & & | \\ K & & G \end{array}$$

Thus N'/K is the smallest Galois extension containing L , so H' is the biggest group contained in H such that H' is normal in G .

Thus H' is the intersection of the G -conjugates of H . Equivalently it is the kernel of $G \rightarrow \text{Sym}(G/H)$ via left multiplication (we did it last semester). Group theory term: $H' := \text{core}_G(H)$.

Previously: We showed a length $\alpha \in \mathbb{R}_{>0}$ is constructible using straightedge and compass if and only if $\mathbb{Q}(\alpha) \subseteq K_n$, where $[K_i : K_{i-1}] = 2$ is a tower of fields with $K_0 = \mathbb{Q}$.

Now show α is constructible if and only if $[\text{Gal. cl. of } \mathbb{Q}(\alpha)/\mathbb{Q} : \mathbb{Q}] = 2^n$. This is the same as saying the splitting field of the minimal polynomial of α over \mathbb{Q} has degree 2^n .

Proof. If α is constructible, then the Galois closure of $\mathbb{Q}(\alpha)/\mathbb{Q}$ is $\mathbb{Q}(\{\sigma(\alpha) \mid \sigma \in \text{Hom}_{\mathbb{Q}}(\Omega, \Omega')\})$ for some suitably large fields Ω, Ω' (for example $\Omega = \Omega' = \mathbb{C}$).

This is contained in the compositum of all $\sigma(K_n)$, of which there are finitely many because K_n/K is finite (so the number of restrictions $\sigma|_{K_n}$ is finite).

This compositum has degree a power of 2, so the Galois closure has degree a power of two (since it's contained in a 2^m degree extension).

The converse follows from some group theory concerning p -groups. Namely, we show any subgroup of a p -group, the normalizer is larger than itself.



Note: Fixed the proof of Proposition IV.6.3 from last time, see the proof there.

Last Time: If $N_1/K, N_2/K$ are Galois, then N_1N_2/K is Galois, and

$$\psi : \text{Gal}(N_1N_2/K) \hookrightarrow \text{Gal}(N_1/K) \times \text{Gal}(N_2/K).$$

Proposition IV.6.9

$N_1 \cap N_2 = K$ if and only if ψ is an isomorphism. That is

$$\text{Gal}(N_1N_2/K) \cong \text{Gal}(N_1/K) \times \text{Gal}(N_2/K).$$

Proof. We see that

$$\text{Gal}(N_1N_2/N_1) \cong \text{Gal}(N_2/(N_1 \cap N_2))$$

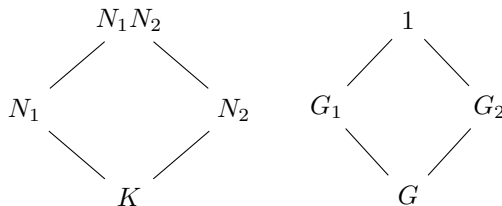
with restriction being the map by Proposition IV.6.3. This equals $\text{Gal}(N_2/K)$ if and only if $N_1 \cap N_2 = K$ by the Galois correspondence.

This proves the result, since it says that $\text{im } \psi$ contains $1 \times \text{Gal}(N_2/K)$ if and only if $N_1 \cap N_2 = K$.

Which then of course holds if and only if it contains $\text{Gal}(N_1/K) \times 1$. Together, these generate the group, so we're done, as ψ is now surjective if and only if $N_1 \cap N_2 = K$, and a priori we have ψ is injective.



Another Perspective. Alternatively, let $G := \text{Gal}(N_1N_2/K)$, $G_i := \text{Gal}(N_1N_2/N_i)$.



Now $G_1 \cap G_2 = 1$ because if you fix N_1, N_2 you must fix N_1N_2 .

By Galoisness, we know $G_1, G_2 \trianglelefteq G$ (normal subgroups). Then $N_1 \cap N_2 = K$ if and only if $\langle G_1, G_2 \rangle = G$.

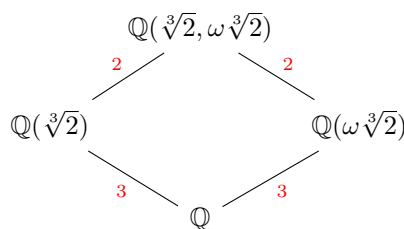
But then $\langle G_1, G_2 \rangle = G_1 \times G_2$.



Corollary IV.6.10


If $N_1 \cap N_2 = K$, then $[N_1N_2 : K] = [N_1 : K][N_2 : K]$ when $N_1/K, N_2/K$ are Galois.

Note: Let $\omega = e^{2\pi i/3}$. Then even though $\mathbb{Q}(\sqrt[3]{2}) \cap \mathbb{Q}(\omega\sqrt[3]{2}) = \mathbb{Q}$ we have



Corollary IV.6.11 (to Proposition IV.6.3)

If N/K is Galois and L/K is arbitrary then $[NL : L] \mid [N : K]$.

Proof. $[NL : L] = \# \text{Gal}(NL/L) = \# \text{Gal}(N/(N \cap L))$ which divides $\text{Gal}(N/K)$ by Lagrange's theorem. 

Lemma IV.6.12

For any extensions M/K and L/K , we have that

$$[ML : M] \leq [L : K].$$

Proof. If $L = K(\alpha)$, then $[L : K]$ is the degree of the minimal polynomial $f(X)$ of α over K .

But then $f(X) \in M[X]$ and $f(\alpha) = 0$, so if $g(X)$ is the minimal polynomial of α over M then $g \mid f$.

But then $ML = M(\alpha)$, so $[ML : M] = \deg g \leq \deg f = [L : K]$, with equality if and only if f remains irreducible in $M[X]$.


In general, we can proceed by induction, letting $L = K(\alpha_1, \dots, \alpha_n)$ and exploiting multiplicativeness of degrees in towers.

Then we have for $M_i = M(\alpha_1, \dots, \alpha_i)$, $K_i = K(\alpha_1, \dots, \alpha_i)$ that

$$[ML : M] = \prod_{i=2}^n [M_i : M_{i-1}] \leq \prod_{i=2}^n [K_i : K_{i-1}] = [L : K].$$



Alternative Proof. Take a basis ℓ_1, \dots, ℓ_n for L over K . Then $V = \text{span}_M(\ell_1, \dots, \ell_n)$ contains M, L , and is a ring (fairly easy to show).

Since it is finite-dimensional over M , it is in fact a field. And so it contains the compositum ML , and is clearly contained in ML . Thus it is ML , showing the fact immediately. 

Last Time: If $\alpha \in \mathbb{R}$ is constructible by straightedge and compass, then α is algebraic and α is contained in a field K_n which is the top of some tower of degree 2 extensions.

And even better, we can take K_n/\mathbb{Q} to be Galois.

Now we'll prove the converse. Suppose $\alpha \in \mathbb{R}$, $\alpha \in N$, N/\mathbb{Q} is Galois, and $[N : \mathbb{Q}] = 2^n$.

Lets show that there exists a tower of degree two extensions $L_0 := \mathbb{Q}(\alpha)$, $L_k = \mathbb{Q}$, $[L_{i-1} : L_i] = 2$.

Proof. In group language using Galois theory. It suffices to show that if G is a 2-group of order 2^n , and $H < G$, then there exists a J such that $H < J \leq G$ and $[J : H] = 2$. We'd then take $G := \text{Gal}(N/\mathbb{Q})$, $H := \text{Gal}(N/L_{i-1})$, and set $L_i = N^J$ to induct.

We'll show this more generally for p -groups where p is a prime. Let $|G| = p^n$, $H < G$. Then there exists a J with $H < J \leq G$ and $[J : H] = p$, and in fact H is normal in J .

This implies that $N_G(H) \supsetneq H$, since $J \subseteq N_G(H)$. Conversely, if $N_G(H) \supsetneq H$, then $N_G(H)/H$ is a p -group, so it has some order p subgroup J' . This corresponds to a subgroup $H < J \leq N_G(H) \leq G$ such that $[J : H] = p$.

This means we can equivalently show that $N_G(H) \supsetneq H$. If $H = 1$, then $N_G(H) = G$ and we're done. So suppose $H \neq 1$.

To show this, note that $g \in N_G(H)$ if and only if $g^{-1}hg \in H$ for every $h \in H$. That is if and only if $hg \in gH$ for every $h \in H$, or $hH = gH$ for every $h \in H$.

Thus it suffices to show there is a coset of H which is fixed under multiplication on the left by H other than H . Call this action $\rho : H \rightarrow \text{Sym}(G/H)$, and we're looking for a fixed point. We see that for any $gH \in \text{Sym}(G/H)$

$$|\text{Orbit}(gH)| = \frac{|H|}{|\text{Stab}(gH)|} = p^i$$

for some i , because $\text{Stab}(gH) \leq H \leq G$. Then G/H is zero mod p , and $|\text{Orb}(gH)|$ is zero mod p unless $i = 0$. Thus since H is a fixed point, to get zero mod p we must have other fixed points.

This completes the proof



Definition IV.6.6

L/K is called normal if $\text{Hom}_K(L, M) = \text{Aut}_K(L)$ for every $M \supseteq L$.

Recall IV.6.3

L/K is Galois if $|\text{Aut}_K(L)| = [L : K]$, and L/K is separable if $|\text{Hom}_K(L, M)| = [L : K]$ for some field $M \supseteq K$ (M needs to be large enough).

L/K Galois implies L/K is separable.

L/K is Galois if and only if L is the splitting field over K of some separable $f(X) \in K[X]$.

L/K is Galois if and only if L/K is separable and normal.

How do we deal with non-Galois extensions? If L/K is separable, let N/K be the Galois closure of L/K (write L as $K(\alpha)$ and split the minimal polynomial of α). Then letting $G := \text{Gal}(N/K)$, $H := \text{Gal}(N/L)$. Then fields between L and K correspond to groups between G and H (see HW10).

Note that this can be studied by the action of G on G/H by left multiplication, and the kernel is trivial because any kernel would give a Galois extension between N and L .

Given a separable extension L/K , we can write $L = L_n \supseteq L_{n-1} \supseteq \cdots \supseteq L_0 = K$ where there is no field between L_i and L_{i-1} . This is a powerful approach, enabling one to study arbitrary extensions L/K via inducting, with inductive step addresses only minimal extensions (see HW9, does not work for Q3).

Useful because: Galois groups of (Galois closures of) minimal separable extensions are massively constrained.

Definition IV.6.7

Call such a Galois group of the Galois closure of a minimal separable extension a primitive permutation group

(viewed as a permutation group by the action of G on G/H).

Facts:

- If G is a primitive subgroup of S_n , then either
 - $L \times L \times \cdots \times L \leq G \leq \text{Aut}(L^k) = (\text{Aut}(L))^k \rtimes S_k$ where L is a nonabelian simple group.
 - $n = p^k$, p prime, $(\mathbb{F}_p)^k \leq G \leq \text{AGL}_k(\mathbb{F}_p)$.

Where

$$\text{AGL}_k(\mathbb{F}_p) = (\mathbb{F}_p)^k \rtimes \text{GL}_k(\mathbb{F}_p)$$

in the usual action on $(\mathbb{F}_p)^k$.

- Also for 100% (not all) of positive integers n , the only primitive subgroups of degree n are A_n and S_n .
- Also if n is prime, then every transitive subgroup of S_n is
 - S_n or A_n
 - groups between \mathbb{F}_n and $\text{AGL}_1(\mathbb{F}_n)$.
 - If $n = (q^k - 1)/(q - 1)$ with $k \geq 2$, and q a prime power, then groups

$$\text{PGL}_k(\mathbb{F}_q) \leq G \leq \text{P}\Gamma\text{L}_k(\mathbb{F}_q)$$

acting on $\mathbb{P}^{k-1}(\mathbb{F}_q)$ (the projective plane).

- if $n = 23$, there's M_{23} (Mathieu simple group).
- If $n = 11$, you get M_{11} and $\text{PSL}_2(\mathbb{F}_{11})$.

IV.7. Solvability by Radicals

Given $f(X) \in \mathbb{Q}[x] \setminus \mathbb{Q}$, when can all roots of $f(X)$ be expressed in terms of nested radicals, e.g.,

$$\sqrt[3]{57\sqrt{31} - 53\sqrt[5]{21 + \sqrt{3}}}$$

Definition IV.7.1

An element $\alpha \in \mathbb{C}$ is expressible in terms of nested radicals if and only if $\alpha \in K_n$ for some field K_n such that $K_n \supseteq K_{n-1} \supseteq \cdots \supseteq K_0 = \mathbb{Q}$ such that

$$K_i = K_{i-1}(\alpha_i) \text{ with } \alpha_i^{d_i} \in K_{i-1} \text{ for some positive integer } d_i.$$

We call a polynomial $f(X) \in \mathbb{Q}[X] \setminus \mathbb{Q}$ solvable by radicals provided that all its complex roots are expressible in terms of nested radicals.

This is equivalent to the splitting field of $f(X)$ over \mathbb{Q} being contained in such a field K_n (by pasting towers together).

Theorem IV.7.1

For any separable $f(X) \in \mathbb{Q}[X] \setminus \mathbb{Q}$, $f(X)$ is “solvable by radicals” if and only if $\text{Gal}(f/\mathbb{Q})$ (that is the Galois group of the splitting field)


is “solvable,” i.e., the Jordan Hölder decomposition

$$\text{Gal}(f/\mathbb{Q}) \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_k = 1$$

where G_{i-1} is normal in G_i and G_i/G_{i-1} is cyclic of prime order.

Proposition IV.7.2

Abelian groups are solvable.

Proof. Every group in the Jordan Hölder decomposition is simple and abelian, and the only such groups are cyclic of prime order. 

Corollary IV.7.3

All polynomials in $\mathbb{Q}[X]$ of degree ≤ 4 are solvable by radicals, since all subgroups of S_1, S_2, S_3, S_4 are solvable.

But for all $n \geq 5$, there exist degree n irreducible $f(X) \in \mathbb{Q}[X]$ that are not solvable by radicals, namely because there exist $f(X)$ with $\text{Gal}(f/\mathbb{Q}) \cong S_n$, which is not solvable because A_n is simple for $n \geq 5$.

Proof of Theorem IV.7.1, part one. Suppose $f(X)$ is solvable, then we wish to show $G := \text{Gal}(f(X), \mathbb{Q})$ is solvable.

Let the splitting field of $f(X)$ be given by K_n , where $K_n \supseteq K_{n-1} \supseteq \cdots \supseteq K_0 = \mathbb{Q}$, and $K_i = K_{i-1}(\alpha_i)$ where $\alpha_i^{d_i} \in K_{i-1}$, $d_i \in \mathbb{Z}_{>0}$.

We may assume that every d_i is prime since

$$K(\alpha^{1/ab}) = (K(\alpha^{1/a})) \left((\alpha^{1/a})^{1/b} \right).$$

We may also assume that K_n contains all complex N -th roots of unity, for any fixed N .

Thus we may assume all roots of $f(X)$ are in a field K_n where $K_{-1} = \mathbb{Q}$, $K_0 = \mathbb{Q}(e^{2\pi i/N})$, $K_i = K_{i-1}(\alpha_i)$ for $i \geq 1$, $\alpha_i^{d_i} \in K_{i-1}$, d_i prime, $d_i \mid N$.

We'll show for all $i > 1$, either $K_i = K_{i-1}$ or K_i/K_{i-1} is Galois with group C_{d_i} . Thus suppose $\alpha_i \notin K_{i-1}$ (if $\alpha_i \in K_{i-1}$ we have $K_i = K_{i-1}$).

Claim

Write $p := d_i$. We're trying then to show that if L contains a primitive p -th root of unity ζ and an element α of some extension of L satisfies $\alpha^p \in L$, but $\alpha \notin L$, then $X^p - \alpha^p$ is irreducible in $L[X]$. Even better, $\text{Gal}(X^p - \alpha^p, L) \cong C_p$.

Why? Roots of $X^p - \alpha^p$ are exactly $\alpha\zeta^i$ for $i = 0, 1, \dots, p-1$, which is Galois. The splitting field of $X^p - \alpha^p$ over L is $L(\alpha)$, so $L(\alpha)/L$ is Galois. Let σ be any non-identity element of $\text{Gal}(L(\alpha)/L)$, which exists since $[L(\alpha) : L] > 1$. Then σ cannot fix α .

Therefore $\sigma(\alpha) = \alpha\zeta^i$ for $1 \leq i \leq p-1$. Because p is prime, ζ^i has order p , write it as ξ , as there is no need to distinguish a p -th root of unity. Then σ fixes $\xi = \zeta^i \in L$. Then

$$\alpha \xrightarrow{\sigma} \alpha\xi \xrightarrow{\sigma} \alpha\xi^2 \xrightarrow{\sigma} \alpha\xi^3 \mapsto \cdots$$

This cycles once we've applied σ p times. Thus σ has order p , and $|\text{Gal}(L(\alpha)/L)| = [L(\alpha) : L] \leq p$ because α satisfies $X^p - \alpha^p \in L[X]$. Therefore $\text{Gal}(L(\alpha)/L) = \langle \sigma \rangle \cong C_p$. This implies $X^p - \alpha^p$ is irreducible, as it is the minimal polynomial of α .

Perfect!

Note we have previously shown $\mathbb{Q}(e^{2\pi i/N})/\mathbb{Q}$ is Galois.

Note: We can make K_n/\mathbb{Q} Galois with group G , namely, the Galois closure is given by the compositum of $\sigma(K_n)$ for homomorphisms $\sigma \in \text{Hom}_{\mathbb{Q}}(K_n, \mathbb{C})$, and these all can be built in the same way as K_n , and then pasted together.

Then we have a picture

$$\begin{array}{ccc}
 K_n & & G_n \\
 | & & | \\
 \vdots & & \vdots \\
 K_2 = K_1(\alpha_2) & & G_2 \\
 | & & | \\
 K_1 = K_0(\alpha_1) & & G_1 \\
 | & & | \\
 K_0 = \mathbb{Q}(e^{2\pi i/N}) & & G_0 \\
 | & & | \\
 K_{-1} = \mathbb{Q} & & G_{-1} = G
 \end{array}$$

where $K_i = K_{i-1}$ or K_i/K_{i-1} is Galois with Galois group cyclic of prime order. Thus $G_i \trianglelefteq G_{i-1}$ with $G_{i-1}/G_i \cong C_p$ for a prime p or $p = 1$. At least for $i \geq 1$. For K_0/K_{-1} , this is Galois with Galois group $(\mathbb{Z}/N\mathbb{Z})^\times$, which is abelian, so this is a fine decomposition.

We started with $f(X) \in \mathbb{Q}[X]$ with splitting field L (over \mathbb{Q}). We've shown there exists N such that $G := \text{Gal}(L(e^{2\pi i/N})/\mathbb{Q})$ is solvable.

Now conclude that $\text{Gal}(L/\mathbb{Q}) = G/H$ for $H := \text{Gal}(L(e^{2\pi iN})/L)$ is solvable.

Namely if $\pi : G \rightarrow G/H$ is the quotient map then

$$G/H = \pi(G) \supseteq \pi(G_0) \supseteq \pi(G_1) \supseteq \cdots \supseteq \pi(G_n) = 1.$$

Then we see that

$$G_{i-1} \twoheadrightarrow \pi(G_{i-1}) \twoheadrightarrow \pi(G_{i-1})/\pi(G_i)$$

the kernel contains G_i so

$$G_{i-1}/G_i \twoheadrightarrow \pi(G_{i-1})/\pi(G_i).$$

The left side has prime order or order 1, so $\pi(G_{i-1})/\pi(G_i)$ has order 1 or p .

Thus $\text{Gal}(f(X), \mathbb{Q}) = G/H$ is solvable.



Lemma IV.7.4 (Key lemma)

If a field L contains n n -th roots of unity, and N/L is Galois with $\text{Gal}(N/L) \cong C_n$, then $N = L(\alpha)$ where $\alpha^n \in L$.

Proof. Of course L contains a primitive n -th root of unity, because the multiplicative group of the n -th roots of unity in L is cyclic.

See Piazza for a proof



Proof of Theorem IV.7.1, part two. If $f(X) \in \mathbb{Q}[X] \setminus \mathbb{Q}$ and $\text{Gal}(f/\mathbb{Q})$ is solvable, then we must show $f(X)$ is solvable.

Then we have that the splitting field K_n of f/\mathbb{Q} is given as a tower $K_n \supseteq \cdots \supseteq K_1 \supseteq K_0 = \mathbb{Q}$ with K_i/K_{i-1} Galois with prime degree.

Say $[K_i : K_{i-1}] = p$, for p a prime. Consider $L = K_{i-1}(e^{2\pi i/p})$. Then LK_i/L is Galois, with group a subgroup of $\text{Gal}(K_i/K_{i-1}) \cong C_p$.

Thus the group is either 1 or C_p . If it's 1, then adjoining a p -th root of unity suffices.

If the group is C_p , the lemma says that $LK_i = L(\alpha)$ for some α where $\alpha^p \in L$. Thus we can adjoin a p -th root of unity as well as α^p .

Thus everything in the splitting field is expressible in radicals.



Example IV.7.1

Let $f(X) = (x-2)(x-4)(x-6)(x^2+2) + 2/N$, where N is large, N is odd, so that $f(X)$ still has three real roots.

Then complex conjugation is a 2-cycle of $f(X)$, and it is irreducible by Eisenstein since

$$N(x-2)(x-4)(x-6)(x^2+2) + 2$$

has coefficients divisible by 2 except the leading term, and $2^2 \nmid 2$.

Thus $\text{Gal}(f/\mathbb{Q})$ is a transitive subgroup of S_5 , so it contains a 5-cycle. Containing a 5-cycle and a 2-cycle is enough to generate S_5 , so $\text{Gal}(f/\mathbb{Q}) = S_5$.

Then of course $f(X)$ is not solvable by radicals.

V. Modules

Definition V.0.1

If R is a ring, an R -module is an abelian group under $+$ equipped with an operation $\cdot : R \times M \rightarrow M$ satisfying

- $r \cdot (r_2 \cdot m) = (r_1 r_2) \cdot m$.
- $r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2$.
- $(r_1 + r_2) \cdot m = r_1 \cdot m + r_2 \cdot m$.
- $1 \cdot m = m$.

If R is a field, then R -module are R -vector spaces

Example V.0.1

\mathbb{Z} -modules are just abelian groups. The last two axioms impose a unique $\cdot : \mathbb{Z} \times M \rightarrow M$.

What are $K[X]$ -modules, for K a field. Well they're automatically K -vector spaces V , along with a distinguished map K -linear map $V \rightarrow V$ given by $m \mapsto x \cdot m$ (this map determines the action of $K[X]$ on V).

An R -module contained in R are exactly ideals of R .

Definition V.0.2

If M is an R -module, then an R -submodule of M is an additive subgroup of M which is closed under multiplication by R .

Definition V.0.3 (Direct Sum Module)

If M, N are R -modules, $M \times N$ is an R -module where the action of R is taken coordinate-wise.

We often denote this $M \oplus N$.

Definition V.0.4

Given a module M and an ideal I of R , then

$$IM = \left\{ \sum_{\ell=1}^n i_{\ell} m_{\ell} : i_{\ell} \in I, m_{\ell} \in M \right\}$$

is an R -module.

Definition V.0.5 (Quotient Modules)

If N is a submodule of an R -module M , then we know M/N is an abelian group under addition.

In fact, M/N is an R -module, where $r \cdot (m + N) = r \cdot m + N$ (check this is well-defined).

Explicitly, if $m + N = m' + N$, then $m - m' \in N$, so $r(m - m') \in N$, so $rm - rm' \in N$, so $rm + N = rm' + N$.

Definition V.0.6

If M, N are R -modules, we call a function $f : M \rightarrow N$ a homomorphism of R -modules if it is a homomorphism of abelian groups such that $f(r \cdot m) = r \cdot f(m)$.

The kernel and image are R -submodules of M, N respectively.

Definition V.0.7

A “free” R -module is the direct sum $R^n := R \oplus R \oplus \cdots \oplus R$.

We call n the “rank” of R^n .

Note: R is a free R -module, and submodules of R are ideals. So

Example V.0.2

If $R = \mathbb{Z}[\sqrt{-5}]$, then R is a free R -module of rank 1. Recall that R has an ideal (aka a submodule) $(2, 1 + \sqrt{-5})$, which is not free. This violates our intuitions!


We’ve proven it’s not free of rank 1, proving it’s not free is a bit harder.

Proposition V.0.1

If R is not the zero ring, and $m \neq n$, then $R^m \not\cong R^n$ (as R -modules).

Proof. Let I be a maximal ideal of R . Suppose $m < n$, and $f : R^m \rightarrow R^n$ is an isomorphism.

Then R^n is spanned by f -images of the standard basis of R^m . Call these $\alpha_1, \dots, \alpha_m$. Thus R^n is R -linear combinations of $\alpha_1, \dots, \alpha_m$.

Then $(R/I)^n$ will be R/I -linear combinations of the images of $\alpha_1, \dots, \alpha_m$ under $R^n \rightarrow (R/I)^n$. But then R/I is a field, $(R/I)^n$ is an R/I -vector space of dimension n , so it cannot be spanned by m elements. 

Next goal: Determine all finitely generated \mathbb{Z} -modules (aka finitely generated abelian groups).

Theorem V.0.2 (Structure Theorem for Abelian Groups)

If G is a finitely generated abelian group, then

$$G \cong \mathbb{Z}^n \oplus \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_r\mathbb{Z}$$

where $n, r \geq 0$, $d_i \in \mathbb{Z}_{>0}$, $d_i \mid d_2 \mid \cdots \mid d_r$.

Also: n, r, d_i 's are uniquely determined.

Proof. Suppose G is a finitely generated abelian group, with generators g_1, \dots, g_m . Consider $\varphi : \mathbb{Z}^m \rightarrow G$ given by

$$(e_1, \dots, e_m) \mapsto e_1g_1 + \cdots + e_mg_m.$$

This is a surjective group homomorphism (since G is abelian). Therefore $G \cong \mathbb{Z}^m / \ker \varphi$. Thus it suffices to understand $\ker \varphi$.

Write $K := \ker(\varphi)$, so K is a subgroup of \mathbb{Z}^m . First we show that K is finitely generated.

Claim

More generally, if R is Noetherian, then any submodule of R^n is finitely generated.

If R is a PID, then the submodule is generated by at most n elements.

If M is a submodule of R^n , consider $\pi_i : R^n \rightarrow R$ which projects onto the i -th coordinate. This is an R -module homomorphism.

So $\pi_1(M)$ is a submodule of R , so $\pi_1(M) = (a_1, \dots, a_m) \subseteq R$ for some $a_1, \dots, a_m \in R$, by Noetherian-ness.

Let $\alpha_{11}, \dots, \alpha_{1m}$ satisfy $\pi_1(\alpha_{1i}) = a_i$.

Then $M = \ker(\pi_1|_M) \oplus R(\alpha_1, \dots, \alpha_n)$. $\pi_1(m) \in (a_1, \dots, a_m)$, so

$$\pi_1(m) = \sum_i r_i a_i = \pi_1 \left(\sum_i r_i \alpha_{1i} \right)$$

Thus $m - \sum_i r_i \alpha_i \in \ker \pi_1$. It is easy to verify uniqueness.

Then $\ker \pi_1|_M$ is a submodule of $\ker \pi_1 \cong R^{n-1}$, so this follows by inducting on n (the base case is given by Noetherian-ness).

Therefore K is a finitely generated subgroup of \mathbb{Z}^m . Say the generators of K are k_1, \dots, k_ℓ . Write $k_i = (k_{i1}, \dots, k_{im})$. Then

$$\begin{bmatrix} k_{11} & k_{12} & \cdots & k_{1m} \\ k_{21} & k_{22} & \cdots & k_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ k_{\ell 1} & k_{\ell 2} & \cdots & k_{\ell m} \end{bmatrix} \cdot \begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_m \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

What operations can we perform on the $[k_{ij}]$ matrix.

- Swapping two rows just means reordering k_1, \dots, k_ℓ .

- Adding a multiple of one row to another (one at a time). By swapping this is exactly the same as replacing row 1 with row 1 plus a times row 2.

This is the same as replacing k_1 by $k_1 + ak_2$, which is fine because $\langle k_1, k_2 \rangle = \langle k_1 + ak_2, k_2 \rangle$.

- Swapping two g_i 's means swapping the columns
- Replacing g_1 by $g_1 + ag_2$ where $a \in \mathbb{Z}$ does not change G (since $\langle g_1, g_2 \rangle = \langle g_1 + ag_2, g_2 \rangle$).

This has the effect of subtracting a times the 1st column from the second column.

- Multiply a column by -1 , multiply a row by -1 .

Proof to be continued next time!



Continued Proof of Theorem V.0.2. We want to use these operations to simplify K .

If K is all zeros, then we're done. Swap columns if needed to make 1st row contain a nonzero matrix entry k_{1i} , and then swap columns to make k_{11} nonzero. We can then multiply 1st row by -1 if needed to make $k_{11} > 0$.

Subtract a multiple of 1st column from second column to make k_{12} satisfy $0 \leq k_{12} < k_{11}$. Similarly in columns $3, 4, 5, \dots, m$

If some $k_{1i} \neq 0$ with $i > 1$, then swap column 1 and column i and repeat until we cannot continue.

At this point we have $k_{11} > 0, k_{12}, \dots, k_{1m} = 0$.

Apply the analogue of this process to the 1st column until $k_{11} > 0, k_{21}, \dots, k_{\ell 1} = 0$.

Now do this process to the rows again. Keep going back and forth, k_{11} is getting smaller and smaller, but remaining positive. Thus this stops after finitely many steps.

At this point, the first row and first column are zero. That is $k_{11} > 0, k_{1j} = k_{i1} = 0, i, j > 1$.

If some k_{ij} is not divisible by k_{11} , add the i -th row to the first—this doesn't change k_{11} , but it makes k_{1j} be not divisible by k_{11} .

Do the previous steps over again until $k_{11} > 0, k_{1j} = k_{i1} = 0$. Repeat these steps, since they reduce k_{11} , they have to terminate eventually.

Thus $k_{11} \mid k_{ij}, k_{11} > 0, k_{1j} = k_{i1} = 0$ for all $i, j > 1$. As an example, we've gotten something like

$$\begin{bmatrix} 3 & 0 & 0 \\ 0 & 6 & 18 \\ 0 & -3 & 21 \\ 0 & 300 & 30 \end{bmatrix}$$

Now do all the same steps to get either $k_{ij} = 0$ for all $i, j > 1$ or $k_{22} > 0, k_{22} \mid k_{ij}, i, j > 2, k_{2j} = k_{i2} = 0$ for $i, j > 2$, and $k_{11} \mid k_{22}$.

Continue this process as long as possible. We end up with a $[k_{ij}]$ matrix looking like

$$\begin{bmatrix} k_{11} & 0 \cdots & 0 \cdots & 0 \\ 0 & k_{22} & \cdots & 0 & \cdots 0 \\ \vdots & \vdots & \ddots & \vdots \\ & \ddots & \vdots \\ 0 & \cdots & \cdots & k_{\ell\ell} & \cdots & 0 \end{bmatrix} \begin{bmatrix} h_1 \\ \vdots \\ h_m \end{bmatrix}$$

where $0 \leq k_{11}, k_{22}, \dots$ and $k_{11} \mid k_{22} \mid k_{33}, \dots$ and the h_i generate G . The relations are then just

$$k_{ii}h_i = 0$$

for all $1 \leq i \leq \ell$. Thus G is \mathbb{Z}^m/K , and K is given as

$$G \cong \mathbb{Z}/(r_1) \oplus \mathbb{Z}/(r_2) \oplus \cdots \oplus \mathbb{Z}/(r_m)$$

where $r_i = k_{ii}$ for $1 \leq i \leq \ell$ and $r_i = 0$ for $i > \ell$, where $r_1, \dots, r_n \geq 0$, $r_1 \mid r_2 \mid r_3 \cdots$. This gives something like

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}.$$

Essentially, we've shown for every matrix $M \in M_{\ell \times m}(\mathbb{Z})$, there exists invertible $P \in \text{GL}_\ell(\mathbb{Z})$, $Q \in \text{GL}_m(\mathbb{Z})$ so that

$$PMQ = \begin{bmatrix} r_1 & 0 & \cdots & 0 & \cdots & 0 \\ 0 & r_2 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & & \\ & & \ddots & 0 & \cdots & r_\ell & \cdots & 0 \end{bmatrix}$$

has the form of a non-negative diagonal matrix with subsequent entries dividing each other.

Now we wish to show G uniquely determines the r_i above which aren't 1. Let T be the group of finite order elements in G . Then $T = \bigoplus_{r_i > 0} \mathbb{Z}/(r_i)$. Then $G/T \cong \bigoplus_{r_i = 0} \mathbb{Z}$. We showed last time $\mathbb{Z}^k \cong \mathbb{Z}^\ell$ implies $k = \ell$.

Thus G/T is uniquely determined, that is the number of i s such that $r_i = 0$. Now consider T , which is

$$T = \mathbb{Z}/(r_1) \oplus \cdots \oplus \mathbb{Z}/(r_q)$$

where $0 < r_1, \dots, r_q$ and $r_1 \mid r_2 \mid \cdots \mid r_q$. We must show T uniquely determines the r_i .

The elements in T of order dividing 2 are


$$\bigoplus_{i=1}^{\ell} \begin{cases} \mathbb{Z}/2\mathbb{Z} & \text{if } r_i \text{ even} \\ 1 & \text{if } r_i \text{ odd} \end{cases}.$$

This tells you the number of even r_i 's. Elements in T of order dividing 4 are

$$\bigoplus_{i=1}^{\ell} \mathbb{Z}/(\gcd(r_i, 4))$$

since T determines the number of even r_i , T determines the # of r_i 's divisible by 4.

Likewise, for every prime power p^a , T determines the number of r_i 's divisible by p^a .

Since $r_1 \mid r_2 \mid \cdots \mid r_\ell$, this determines which r_i 's are divisible by p^a , which gets everything by unique factorization. 

Generalization: If R is a PID and $k_1, k_2 \in R^n$ with $k_{11}, k_{21} \neq 0$. Then we're looking for

$$Rk_1 + Rk_2 = Rk'_1 + Rk'_2$$

where $k'_1 = uk_1 + vk_2$ with $u, v \in R$ where $(uk_{11} + vk_{21}) = (k_{11}, k_{21})$, so $uk_{11} + vk_{21} = \gcd(k_{11}, k_{21})$.

We know u, v are coprime, as $u \frac{k_{11}}{\gcd} + v \frac{k_{21}}{\gcd} = 1$, so what we're doing is

$$\begin{bmatrix} u & v \\ -\frac{k_{21}}{\gcd} & \frac{k_{11}}{\gcd} \end{bmatrix} \cdot \begin{pmatrix} k_1 \\ k_2 \end{pmatrix}$$

so we're setting $k'_2 = \frac{k_{11}}{\gcd} k_2 - \frac{k_{21}}{\gcd} k_1$. Therefore by invertibility of the matrix on the LHS, $Rk_1 + Rk_2 + Rk'_1 + Rk'_2$.

With this, along with the fact that in a Noetherian ring there are no infinite chains of ideals (here principal ideals), we can carry out the same proof as above, as this allows us to say k_{11} cannot reduce forever.

Recall V.0.3

R is Noetherian if and only if every ideal of R is finitely generated.


Theorem V.0.3 (Hilbert Basis Theorem)

if R is Noetherian, then $R[X]$ is Noetherian.

Proof. If I is an ideal of $R[X]$, then the set of leading coefficients in I is an ideal of R .

This is generated by some leading coefficients $\{a_1, \dots, a_r\}$ of polynomials $\{f_1, \dots, f_r\}$.

Also L_n , being the leading coefficients of all $f \in I$, $\deg f = n$ is an ideal of R .

Then I is generated by $\bigcup_{n \leq N} S_n$, where S_n is any finite subset of elements of I with degree whose leading coefficients generate L_n , and where $N = \max_{1 \leq i \leq r} \deg f_i$. 

VI. Symmetric Functions

VI.1. Basics in all Rings

Definition VI.1.1

For any ring R , a polynomial $f(X_1, \dots, X_n) \in R[X_1, \dots, X_n]$ is symmetric if

$$f(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = f(X_1, \dots, X_n)$$

for all $\sigma \in S_n$.

Example VI.1.1

The sum $X_1 + \dots + X_n$ and product $X_1 X_2 \dots X_n$. Also sums of products

$$\sum_{i \neq j} X_i X_j.$$

Consider two variables. Main examples: $X + Y, XY$.

Claim

The symmetric polynomials in $R[X, Y]$ are $R[X + Y, XY]$, that is

$$\{f(X + Y, XY) \mid f(u, v) \in R[u, v]\}.$$

Consider something like this, where we're killing leading terms

$$X^2 + 3XY + Y^2 = (X + Y)^2 + XY.$$

What about degree 3? Ditto!

$$\begin{aligned} X^3 + 5X^2Y + 5XY^2 + Y^3 &= (X + Y)^3 + 2X^2Y + 2XY^2 \\ &= (X + Y)^3 + 2XY(X + Y). \end{aligned}$$

In general, we want to stratify into “homogeneous” pieces

Definition VI.1.2

A nonzero polynomial in $R[X_1, X_2, \dots, X_n]$ is homogeneous of degree m if for each monomial g in f we have

$$m = \sum_{i=1}^n \deg_i g.$$

For nonzero polynomials this says $f(tX_1, \dots, tX_n) = t^m f(X_1, \dots, X_n)$ where $t \in R$.

If $n = 2$, this is like $f(X, Y) = \sum_{i=0}^m a_i x^i y^{m-i}$.

Now any polynomial can be written as the sum of homogeneous polynomials, so we can reduce to this case

Proof. If $f(X, Y) \in R[X, Y]$ is symmetric and homogeneous of degree n , then there exists a monomial $p(U, V) \in R[U, V]$ such that $p(X + Y, XY)$ has the same leading term (sorting by powers of X) as $f(X, Y)$.

Reason: leading term of $f(X, Y)$ is $cx^i y^j$ where $i \geq j$ (by symmetry). So use

$$\begin{aligned} p(U, V) &= cU^{i-j}V^j \\ p(X + Y, XY) &= c(X + Y)^{i-j}(XY)^j = cX^i Y^j + \dots \end{aligned}$$

We see that $p(X + Y, XY)$ is symmetric and homogeneous of degree n since $i + j = n$.

Therefore $f(X, Y) - p(X + Y, XY)$ is symmetric, homogeneous of degree n (or zero), and we’ve lowered the largest power of X which appears. Thus if we continue this process it must terminate.

Namely continue until the difference is the zero polynomial. Conclude if $f(X, Y) \in R[X, Y]$ is symmetric and homogeneous of degree n , then $f(X, Y) = g(X + Y, XY)$ where $g(U, V) \in R[U, V]$

$$g(U, V) = \sum_{i,j} d_{ij} U^i V^j$$

with every $i + 2j = n$.



Theorem VI.1.1 (Symmetric Function Theorem)

The symmetric polynomials in $R[x_1, \dots, x_n]$ are precisely $R[e_1, \dots, e_n]$ where the e_i are the sum of all products of i distinct x_j ’s. Note that

$$\prod_{i=1}^n (T - x_i) = T^n - e_1 T^{n-1} + e_2 T^{n-2} - \dots + (-1)^n e_n.$$

Namely

$$\begin{aligned} e_1 &= x_1 + x_2 + \dots + x_n \\ e_2 &= \sum_{i=1}^n \prod_{i < j} x_i x_j. \end{aligned}$$

For the proof, we use the “lexicographic” ordering of monic monomials. That is we say $x_1^{i_1} \cdots x_n^{i_n}$ comes before $x_1^{j_1} \cdots x_n^{j_n}$ if either $i_1 > j_1$ or $(i_1 = j_1 \text{ and } i_2 > j_2)$ or $(i_1 = j_1, i_2 = j_2 \text{ and } i_3 > j_3)$ or \dots

Key point: There exists only finitely many monic polynomials which are homogeneous of degree d for any prescribed d . Thus we can just follow this procedure above, reducing the X_1 degree, then the X_2 degree, etc.

Proof. Use the same proof as for 2 variables. If $f(x_1, \dots, x_n)$ is symmetric and homogeneous of degree d with leading term $cx_1^{i_1}x_2^{i_2} \cdots x_n^{i_n}$. Note $i_1 \geq i_2 \geq \dots \geq i_n$ (by symmetry).

Note the leading terms of e_j is $x_1 \cdots x_j$. So we subtract of $ce_n^{i_n}$ first, which gives us i_n of all n variables, so we have $cX_1^{i_n} \cdots X_n^{i_n}$. Repeat! This gives us

$$f(x_1, \dots, x_n) - ce_n^{i_n} e_{n-1}^{i_{n-1}-i_n} \cdots e_1^{i_1-i_2}.$$

This is either zero or symmetric and homogeneous of degree d with “smaller” leading term than $f(x_1, \dots, x_n)$.

Repeat until you get zero!

In fact, if we start out homogeneous, everything we end up with is homogeneous!



Example VI.1.2

If $\alpha_1, \dots, \alpha_q$ are the elements of \mathbb{F}_q , and $H(x_1, \dots, x_q) \in \mathbb{F}_q[x_1, \dots, x_q]$ is symmetric and homogeneous of degree $d > 0$.

Then $H(\alpha_1, \dots, \alpha_q) = 0$ when $d < q - 1$. We know that $H(x_1, \dots, x_q) = G(e_1, \dots, e_q)$ for some $G(u_1, \dots, u_q) \in \mathbb{F}_q[u_1, \dots, u_q]$. Furthermore each term of G is $cu_1^{i_1} \cdots u_q^{i_q}$ where

$$i_1 + 2i_2 + 3i_3 + \cdots + qi_q = d.$$

Note then that

$$\prod_{i=1}^q (T - x_i) = T^q - e_1 T^{q-1} + e_2 T^{q-2} - \cdots + (-1)^q e_q$$

$$\prod_{i=1}^q (T - \alpha_i) = T^q - T.$$

Thus

$$0 = e_1(\alpha_1, \dots, \alpha_n) = e_2(\alpha_1, \dots, \alpha_n) = \cdots = e_{q-2}(\alpha_1, \dots, \alpha_n)$$

and $e_q(\alpha_1, \dots, \alpha_n) = 0$. Furthermore $e_{q-1}(\alpha_1, \dots, \alpha_n) = (-1)^{q-1}(-1) = -1$ because q is odd.

Then since we have degree $d < q - 1$, we can't involve any term including e_{q-1} , and so $H(\alpha_1, \dots, \alpha_n) = 0$.

Consequence by breaking into homogeneous parts, if $\alpha_1, \dots, \alpha_q$ are the elements of \mathbb{F}_q and $H(x_1, \dots, x_q) \in \mathbb{F}_q[x_1, \dots, x_q]$ is symmetric of total degree $< q - 1$, then

$$H(\alpha_1, \dots, \alpha_q) = H(0, \dots, 0).$$

Theorem VI.1.2 (Williams, Wan, Turnwald)

If $f(X) \in \mathbb{F}_q[X]$ is nonconstant and $f(\mathbb{F}_q) \neq \mathbb{F}_q$ then

$$\#f(\mathbb{F}_q) \leq q - \frac{q-1}{\deg f}.$$

Proof. First replace $f(X)$ by $f(X) - f(0)$ to assume $f(0) = 0$.

Consider

$$F(X) := \prod_{d \in \mathbb{F}_q} (X - f(d)).$$

Since $f(\mathbb{F}_q) \neq \mathbb{F}_q$ we know $F(X) \neq X^q - X$. Then consider

$$G(X) := F(X) - (X^q - X).$$

This is a nonzero polynomial in $\mathbb{F}_2[X]$. So the total number of roots of G are $\leq \deg(G)$. The # of roots of G in \mathbb{F}_q is exactly $\#f(\mathbb{F}_q)$, so we can get a bound this way.

We see that

$$F(X) = X^q - e_1(f(\alpha_1), \dots, f(\alpha_q))X^{q-1} + e_2(f(\alpha_1), \dots, f(\alpha_q))X^{q-2} - \dots.$$

If $\deg(G) > 1$, then $\deg(G) = q - i$, where i is the smallest positive integer such that

$$e_i(f(\alpha_1), \dots, f(\alpha_q)) \neq 0.$$

Note that $e_i(f(x_1), \dots, f(x_q))$ is symmetric, homogeneous of degree $\leq i \deg(f)$. If $i \deg(f) < q - 1$, then

$$e_i(f(\alpha_1), \dots, f(\alpha_q)) = 0.$$

Thus the minimal i satisfies $i \deg(f) \geq q - 1$. Therefore $i \geq \frac{q-1}{\deg(f)}$.

Wait! We're done! Then

$$\#f(\mathbb{F}_q) \leq \deg G = q - i \leq q - \frac{q-1}{\deg(f)}.$$

If $\deg(G) = 1$, the inequality is trivial.



Appendix A. Gauss's Lemma and its Consequences

Gauss's Lemma and its consequences are critical for our class. However, these were not stated in the best way during class.

In the interest of making my life easier, I have summarized the relevant results here, lifting from Artin and generalizing to the case of an integral domain and its fraction field (as we use this in class and on homework often).

For the remainder of this section, let R be a UFD and $K := \text{Frac}(R)$ be its splitting field.

Definition A.0.1

We define the content of $f \in R[x]$ to be the gcd of its coefficients, so that $f = \text{cont}(f) \cdot \hat{f}$. If $f = 0$ we define $\text{cont}(f) = 1$ for convenience.

We call a polynomial primitive if $\text{cont}(f) = 1$. Clearly \hat{f} is primitive, and we call it the primitive part of f .

We define the content of $g \in K[x]$ to be the following. Let d be the lcm of the denominators of the coefficients of g then $dg \in R[x]$ and

$$\text{cont}(g) = \frac{\text{cont}(dg)}{d}.$$

Note this definition agrees with that in $K[x]$, and

$$g(x) = \text{cont}(g)\hat{g}(x)$$

for $\hat{g}(x) \in R[x]$ primitive (when $\deg g > 0$).

Claim

Useful Fact: If $g(x) \in K[x]$ is monic then $\text{cont}(g)$ is exactly equal to the inverse of the lcm of the denominators of the coefficients of g .

Note this actually holds if any of the coefficients of $g(x)$ are 1, as the position of the coefficients does not impact the content.

Proof. Let d be this least common multiple as above. We must simply show that $\text{cont}(dg) = 1$. Write $g(x) = \sum_{i=0}^n a_i/b_i x^i$ for $a_i, b_i \in R, b_i \neq 0$ coprime. With $a_n/b_n = 1, a_n = b_n = 1$.

Then $\text{cont}(dg) \mid d$ because

$$dg(x) = dx^n + \sum_{i=0}^{n-1} \frac{da_i}{b_i} x^i.$$


Write $d = \text{cont}(dg)r$ for $r \in R$. Then for some $t_i \in R$

$$\begin{aligned} \text{cont}(dg)t_i &= \frac{da_i}{b_i} = \frac{\text{cont}(dg)ra_i}{b_i}. \\ t_i &= \frac{ra_i}{b_i}. \end{aligned}$$

Because $t_i \in R$, this implies that $b_i \mid r$, since a_i, b_i are coprime.

Thus since d is the least common multiple, and r is a multiple, $r = ds$ for some $s \in R$. Then $d = \text{cont}(dg)r = \text{cont}(dg)ds$, so

$$1 = \text{cont}(dg)s$$

so $\text{cont}(dg)$ is a unit, which we may call 1. 

Lemma A.0.1 (Gauss's Lemma)

The product of primitive polynomials is primitive.

As a consequence for any $f, g \in R[x]$

$$\text{cont}(fg) = \text{cont}(f) \cdot \text{cont}(g)$$

because $\hat{f}\hat{g}$ is the primitive part of fg .

Proof. Suppose $p \in R$ is an irreducible factor of the coefficients of fg . That is suppose fg is not primitive.

Then let $\overline{} : R[x] \rightarrow (R/(p))[x]$, noting that $R/(p)$ is an integral domain since (p) is prime. Then

$$0 = \overline{fg} = \overline{f}\overline{g}.$$

Thus one of $\overline{f}, \overline{g} = 0$, so p divides the coefficients of one of f, g . Thus one of f, g is not primitive.

We also see that for any $f, g \in R[x]$ that

$$fg = \text{cont}(f)\hat{f}\text{cont}(g)\hat{g} = \text{cont}(f)\text{cont}(g) \cdot \hat{f}\hat{g}$$

so because $\hat{f}\hat{g}$ is primitive we know that

$$\text{cont}(fg) = \text{cont}(f)\text{cont}(g)$$

$$\hat{f}\hat{g} = \hat{fg}.$$

Proposition A.0.2 (Division of polynomials over K)

If $p(x) \in K[x]$ divides $f(x) \in R[x]$ in $K[x]$ then the primitive part $\hat{p}(x)$ divides $f(x)$ in $R[x]$.


Furthermore, if $f(x) = p(x)q(x)$ then

$$f(x) = a\hat{p}(x)\hat{q}(x)$$

for some $a \in R$. 

Proof. Suppose $p(x)q(x) = f(x)$. Let $\text{cont}(p)\text{cont}(q) = a/b$ for $a, b \in R$ coprime. Then

$$a\hat{p}(x)\hat{q}(x) = bf(x).$$

Then b divides a , since b cannot divide the coefficients of $\hat{p}(x)\hat{q}(x)$ by Lemma A.0.1. Thus $b = 1$ by coprimality, and $\hat{p}(x)(a\hat{q}(x)) = f(x)$. 

Corollary A.0.3

If $f(x) \in R[x]$ can be written as $p_1(x) \cdots p_k(x)$ for $p_i(x) \in K[x]$ then $f(x)$ can be written as

$$f(x) = a\hat{p}_1(x) \cdots \hat{p}_k(x)$$

for $a \in R$.

Proof. This follows from the above since

$$\begin{aligned} f(x) &= a\hat{p}_1(x)p_2(x) \cdots \hat{\cdot} p_k(x) \\ &= a\hat{p}_1(x) \cdots \hat{p}_k(x). \end{aligned}$$

**Proposition A.0.4**

If $f(x) \in R[x]$ is primitive and irreducible then it is irreducible in $K[x]$.

If $g(x) \in K[x]$ is irreducible in $K[x]$ then $\hat{g}(x) \in R[x]$ is irreducible in $R[x]$.

Proof. Let $f(x) = p(x)q(x)$ for $p(x), q(x) \in K[x]$, note that $p(x), q(x) \neq 0$. Then we have for some $a \in R$ that

$$a\hat{p}(x)\hat{q}(x) = f(x).$$

Because f is primitive, $a = 1$, so $\hat{p}(x)$ or $\hat{q}(x)$ is a unit in $R[x]$, so it is a unit in R .

This shows that $p(x) = \text{cont}(p)\hat{p}(x) \in K$ is a unit, so f is irreducible in $K[x]$.

For the second part, note $g(x)$ is a nonzero nonunit in $K[x]$, so $\hat{g}(x) = 1/\text{cont}(g) \cdot g(x)$ is a nonzero nonunit in $K[x]$. Thus it is a nonzero nonunit in $R[x]$.

Write $\hat{g}(x) = p(x)q(x) \mid g$ for $p, q \in R[x]$. Then $p(x)$ is a unit in $K[x]$, so $p = p(x) \in K$. But then p divides the coefficients of $\hat{g}(x)$, so by primitivity p must be a unit in R .

**Proposition A.0.5**

$R[x]$ is a UFD

Proof. Fix $f(x) \in R[x]$. We first show a factorization exists. To do so, recall that $K[x]$ is a PID, so it is a UFD. Thus

$$\begin{aligned} f(x) &= p_1(x) \cdots p_m(x) \\ f(x) &= a\hat{p}_1(x) \cdots \hat{p}_m(x) \end{aligned}$$

for irreducible $p_1, \dots, p_m \in K[x]$, $a \in R$. Then writing $a = a_1 \cdots a_n$ as the prime factorization of $a \in R$ we see that

$$f(x) = a_1 \cdots a_n \hat{p}_1(x) \cdots \hat{p}_m(x)$$

is a prime factorization of $f(x) \in R[x]$.

For uniqueness, if we have

$$a_1 \cdots a_n \hat{p}_1(x) \cdots \hat{p}_m(x) = b_1 \cdots b_k \hat{q}_1(x) \cdots \hat{q}_\ell(x) \cdot \hat{p}_1(x) \cdots \hat{p}_m(x) = \frac{b_1 \cdots b_k}{a_1 \cdots a_n} \hat{q}_1(x) \cdots \hat{q}_\ell(x).$$

Then we have that $m = \ell$ since $K[x]$ is a UFD, and after reordering $\hat{p}_i(x) = c_i \hat{q}_i(x)$ for $c_i \in K^\times$. By primitivity of $\hat{p}_i(x)$, $c_i \in R$ is a unit.

Then cancelling p_i, q_i we have that $a_1 \cdots a_n = ub_1 \cdots b_k$ up to a unit $u \in R$. But then $n = k$ and a_i, b_i differ up to a unit after reordering because R is a UFD.

This proves uniqueness!



Appendix B. The Primitive Element Theorem

Theorem B.0.1 (Primitive Element Theorem)

Let L/K be a finite separable extension. Then $L = K(\alpha)$ for some $\alpha \in L$, and we call α a primitive element for L .

Proof when K is finite. If K is finite, then L is a finite field. From Homework 8 we know that L^\times , being a finite subgroup of itself, is cyclic, say with generator $\alpha \in L^\times$. Then clearly $L = K(\alpha)$ as desired.



Proof when K is infinite. Write $L = K(\alpha_1, \dots, \alpha_r)$ and $L_i = K(\alpha_1, \dots, \alpha_i)$. We will show by induction that L_i has the form $K(\beta_i)$ for some $\beta_i \in L_i$.

The base case $i = 1$ is immediate. Now suppose the result holds for i , then $L_{i+1} = K(\beta_i, \alpha_{i+1})$. For convenience let $\alpha := \alpha_{i+1}, \beta := \beta_i$.

Let $\sigma_1, \dots, \sigma_n$ be the K -homomorphisms $L_{i+1} \rightarrow N$ where N is large enough (for example, we can say N is the splitting field over K of the product of $\text{minpoly}_K(\alpha), \text{minpoly}_K(\beta)$).

Then we know that since L/K is separable that $n = [L : K]$. We will show all but finitely many $c \in K$ satisfy $L = K(\alpha + c\beta)$, so since K is infinite we're done.

Write $\gamma := \alpha + c\beta$. Since $K \subseteq K(\gamma) \subseteq L_{i+1}$, we have $K(\gamma) = L_{i+1}$ if and only if $[K(\gamma) : K] = n$. That is, if and only if the minimal polynomial of γ over K has degree n , which means that it has n distinct roots in a big enough field by separability.

For every root γ' of this polynomial, there is a K -homomorphism $K(\gamma) \rightarrow K(\gamma')$ mapping $\gamma \mapsto \gamma'$, and we can extend this to a homomorphism whose domain is L , which is one of the σ_i .

Thus the roots of the minimal polynomial are $\sigma_i(\gamma)$. Thus $K(\gamma) = L$ if and only if $\sigma_i(\gamma) \neq \sigma_j(\gamma)$ whenever $i \neq j$. This condition says that

$$\sigma_i(\alpha) + c\sigma_i(\beta) \neq \sigma_j(\alpha) + c\sigma_j(\beta).$$

This holds for all $i \neq j$ if and only if c is NOT a root of

$$h(X) := \prod_{i \neq j} (\sigma_i(\alpha) + \sigma_i(\beta)X - \sigma_j(\alpha) - \sigma_j(\beta)X).$$

Note that h is not the zero polynomial, as if it were then $\sigma_i(\alpha) = \sigma_j(\alpha), \sigma_i(\beta) = \sigma_j(\beta)$, and so $\sigma_i = \sigma_j$ on $K(\alpha, \beta) = L_{i+1}$.

Thus h is nonzero, and only has finitely many roots. Thus all but finitely many $c \in K$ satisfy $h(c) \neq 0$, so that $K(\alpha + c\beta) = L_{i+1}$.

This completes the inductive step.

