Fields and Galois Theory

math 370, yale university, spring 2019

These are lecture notes for math 370b, "Fields and Galois Theory," taught by Asher Auel at Yale University during the spring of 2019. These notes are not official, and have not been proofread by the instructor for the course. They live in my lecture notes respository at

https://github.com/jopetty/lecture-notes/tree/master/MATH-370.

If you find any errors, please open a bug report describing the error and label it with the course identifier, or open a pull request so I can correct it.

Contents

Syllabus

Instructor	Asher Auel, asher.auel@yale.edu
Lecture	TR 11:35 AM – 12:50 PM in LOM 215
Peer Tutor	Arthur Azvolinsky, arthur.azvolinsky@yale.edu
Section	Math Lounge
Exams	Midterm 1: Febuary 19; Midterm 2: April 9; Final: May 3.
Textbook	James S. Milne. *Fields and Galois Theory (v4.60)*. 2018

The main object of study in Galois theory are roots of single variable polynomials. Many ancient civilizations (Babylonian, Egyptian, Greek, Chinese, Indian, Persian) knew about the importance of solving quadratic equations. Today, most middle schoolers memorize the "quadratic formula" by heart. While various incomplete methods for solving cubic equations were developed in the ancient world, a general "cubic formula" (as well as a "quartic formula") was not known until the 16th century Italian school. It was conjectured by Gauss, and nearly proven by Ruffini, and then finally by Abel, that the roots of the general quintic polynomial could not be solvable in terms of nested roots. Galois theory provides a satisfactory explanation for this, as well as to the unsolvability (proved independently in the 19th century) of several classical problems concerning compass and straight-edge constructions (e.g., trisecting the angle, doubling the cube, squaring the circle). More generally, Galois theory is all about symmetries of the roots of polynomials. An essential concept is the field extension generated by the roots of a polynomial. The philosophy of Galois theory has also impacted other branches of higher mathematics (Lie groups, topology, number theory, algebraic geometry, differential equations).

This course will provide a rigorous proof-based modern treatment of the main results of field theory and Galois theory. The main topics covered will be irreducibility of polynomials, Gauss's lemma, field extensions, minimal polynomials, separability, field automorphisms, Galois groups and correspondence, constructions with ruler and straight-edge, theory of finite fields. The grading in Math 370 is very focused on precision and correct details. Problem sets will consist of a mix of computational and proof-based problems.

Your final grade for the course will be determined by

$$\max\left\{\begin{array}{l} 20\% \text{ homework} + 25\% \text{ midterm } 1 + 25\% \text{ midterm } 2 + 30\% \text{ final} \\ 20\% \text{ homework} + 25\% \text{ midterm } 1 + 15\% \text{ midterm } 2 + 40\% \text{ final} \\ 20\% \text{ homework} + 15\% \text{ midterm } 1 + 25\% \text{ midterm } 2 + 40\% \text{ final} \end{array}\right\}.$$

References

[Mil18] James S. Milne. *Fields and Galois Theory (v4.60)*. 2018.

1 January 15, 2019

> "Daddy, the bears is wubbing his back!"
>
> Noah Auel

Asher's kids came up and they are soooooo cuuuuuuttteeeeee! That's so adorable. He also says that the course is really fun but honestly the kids are by far my favorite part of the course so far. Hi Noah! Sorry your great-grandfather died :(

1.1 What is Galois Theory?

Galois theory is an explanation of a trajectory we started in grade school. We start with the positive integers $\mathbf{Z}_{>0}$ and we learn to make bijections (bijections between apples on the table and positive integers). Then we discovered (or invented) the concept of zero which led us to $\mathbf{N}$. Then we started using negative numbers to arrive at $\mathbf{Z}$, and from there on to $\mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}$ and so on. Each jump is necessitated by wanting or needing to solve some kind of equation. Galois theory mainly focuses on that last jump from $\mathbf{R}$ to $\mathbf{C}$.

1.2 Moving from $\mathbf{R}$ *to* $\mathbf{C}$

We usually think of $\mathbf{C}$ in the presentation of $\mathbf{C} = \mathbf{R}[i] = \{x + iy \mid x, y \in \mathbf{R}\}$. This value i is a root of the equation $x^2 + 1$, one we can't solve with just real numbers. One could ask "what is so special about this polynomial?" Why is i the thing that builds complex numbers? What about $x^2 + x + 1$? That is also rather fundamental, with roots $\omega = (-1 \pm \sqrt{-3})/2$. If you draw the unit circle in the complex plane, these roots divide the circle into three pieces along with $(1, 0)$. We could form an object $\mathbf{R}[\omega]$ and call that the complex numbers. We don't use this construction because $\mathbf{R}[\omega] = \mathbf{C}$, since

$$x + y\left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) = \left(x - \frac{1}{2}y\right) + \frac{\sqrt{3}}{2}yi,$$

by associativity via the substitution $x' = x - \frac{1}{2}y$ and $y' = \frac{\sqrt{3}}{2}y$. These transformations are always solvable, so the two systems are in fact equivalent.

> **Exercise 1.1.** Let $f : x \mapsto ax^2 + bx + c$ where $a, b, c \in \mathbf{R}$ where $b^2 - 4ac < 0$. Prove that $\mathbf{C} = \mathbf{R}[\alpha]$ where α is a root of f.

But even if you do choose to ordain $x^2 + 1$ as special, there's still nothing special about i since it factors into $(x + i)(x - i)$. Then there are really two roots, $+i$ and $-i$. We have arbitrarily chosen i over $-i$, probably because it was invented by nineteenth century German mathematicians living in the Northern Hemisphere. Algebraically, there is no way to distinguish between i and $-i$. However moving *between* the roots is special: it's a map $\sigma\colon \mathbf{C} \to \mathbf{C} : x + iy \mapsto x - iy$ called an $\mathbf{R}$-automorphism of $\mathbf{C}$, meaning that restricting σ to $\mathbf{R}$ is the identity. It's also a (unital) ring homomorphism, so $\sigma(z_1 + z_2) = \sigma(z_1) + \sigma(z_2)$ and $\sigma(z_1 \cdot z_2) = \sigma(z_1) \cdot \sigma(z_2)$ and $\sigma(1) = 1$.

There are more such automorphisms! We already saw that we can write complex numbers as $\mathbf{C} = \mathbf{R}[\omega]$. We could create the map $\sigma\colon x + y\omega \mapsto x + y\bar{\omega}$. Notice that all these automorphisms are doing is exchanging the roots of the generating polynomials. We can check that this is in fact a valid automorphism by look at what it does to i.

$$\sigma\colon i = \frac{1}{\sqrt{3}} + \frac{2}{\sqrt{3}}\omega \mapsto \frac{1}{\sqrt{3}} + \frac{2}{\sqrt{3}}\bar{\omega} = -i,$$

so it's actually just complex conjugation! In fact, $\mathrm{Aut}_{\mathbf{R}}(\mathbf{C}) = \{\mathrm{id}_{\mathbf{C}}, \sigma\}$.

Example 1.1. Notice that $|\mathrm{Aut}_{\mathbf{R}}(\mathbf{C})| = 2 = \dim_{\mathbf{R}} \mathbf{C} = [\mathbf{C} : \mathbf{R}]$. We'll be seeing a lot of this later.

This shows that the special part of the complex numbers is not i or ω, but rather complex conjugation. This is actually the defining property of the complex numbers irrespective of how you define them.

Proposition 1.1. *More generally, given a field F and a polynomial $f(x) = ax^2 + bx + c$ for some $a, b, c \in F$ satisfying $f(x)$ has no root in F then there exists a field k with the following properties:*

1. *F is a subfield of k;*
2. *$\dim_F k = [k : F] = 2$;*
3. *$|\mathrm{Aut}_F\, k| = 2$; and*
4. *the polynomial f is separable which for us means that $b^2 - 4ac \neq 0$. This is called the quadratic extension of F.*

This will lead us to a new σ which will exchange the roots analogously to conjugation. We'll also need that the characteristic of F is not 2, since otherwise the quadratic formula doesn't work since we divide by $2a$. Implicit in the quadratic formula is the statement that $k = F[\sqrt{b^2 - 4ac}]$.

1.3 Going Cubic

We have a similar story for cubic equations where $f(x) = x^3 + px - q$ (the negative is there for historical reasons). This also leads us to the cubic formula. The Babylonians discovered the quadratic formula, and Italian mathematicians in the 16^{th} century developed the cubic formula,

seriously, just look it up.

because they had these betting games where two mathematicians had to compete to find the roots of a cubic equation. Eventually, a guy named Cardano and his students started winning everything and then one of his students defected to a competitor. The important part is that this formula is a nested formula of certain finitely many operations depending just on the coefficients. There is a similar story for quartic equations.

Theorem 1.2 (Abel-Ruffini)**.** *Given a general polynomial $f \in \mathbf{Q}[x]$ with $\deg(f) \geq 5$, there is no explicit closed form formula for the roots of f only depending on taking nested roots.*

Galois theory is about understanding polynomials by looking at the symmetry of their roots.

2 January 17, 2019

"This is true by the Freshma—First Year's Dream"

Asher

2.1 Reminders from MATH 350

1. F is a field, or a commutative unital ring where every $F^\times = F \setminus \{0\}$.
2. $F[x]$ is the ring of polynomials with coefficients in F.
3. $\partial : F[x] \to \mathbf{N}$ is the degree function. We know that $\partial(fg) = \partial(f) + \partial(g)$ and $\partial(f+g) \le \max\{\partial(f), \partial(g)\}$. Because of multiplicativity, we know that $F[x]^\times$ are nonzero constant polynomials.

Theorem 2.1. *Given a field F, we know that $F[x]$ is a Euclidean Doman with respect to ∂. That us, given $f, g \in F[x]$ where $g \neq 0$, there exist $q, r \in F[x]$ such taht $f = q \cdot g + r$ where either $r = 0$ or $\partial(r) < \partial(g)$.*

Theorem 2.2. *Every Euclidean Doman is a Principal Ideal Domain.*

Definition (Ideal)**.** A subset $I \subset R$ of a ring is an ideal if I is a subring and it is closed under multiplication, so that $rI \subset I$ for every $r \in R$ (we implicitly assume that R is commutative here). Any ideal which contains a unit is the whole ring. *Ideal*

Definition (Principal Ideal)**.** An ideal $I \subset R$ is principal if it is generated by one thing, so $I = (r) = rR$ for some $r \in R$, *Principal Ideal*

Corollary 2.3. *$F[x]$ is a PID. If $I = (f)$ then $I = (cf)$ for some $c \in F^\times$, so we choose our polynomials to be* monic.

Corollary 2.4. *The set of all ideals $\{I \subseteq F[x]\}$ is in bijection with the set of monic polynomials $\{f \in F[x]\}$.*

Definition (Prime Idea)**.** An ideal $I \subseteq R$ is prime if $ab \in I$ implies that either a or b is an element of I. Equivalently, this says that R/I is an integral domain. *Prime Idea*

Definition (Maximal Ideal)**.** An ideal $I \subseteq R$ is maximal if $I \subseteq J \subseteq R$ then either $I = J$ or $J = R$. Equivalently, R/I is a field, so there are no nonzero nonunit elements of R/I. *Maximal Ideal*

Example 2.1 (Ideals in $\mathbf{Z}$)**.** A prime ideal I in $\mathbf{Z}$ is either (0) or (p) for some prime p. In any integral domain, (0) is prime. The only maximal ideals in $\mathbf{Z}$ are (p) by Bezout's Theorem.

Definition (Prime and Irreducible Elements)**.** An element r in R is prime if (r) is prime, or if r divides ab then r divides either a or b. An element r is irreducible if $r = ab$ then $a \in R^\times$ or $b \in R^\times$. Primality always implies irreducibility, but the converse only holds in PIDs.

Prime and Irreducible Elements

Lemma 2.5. *If R is a PID then every irreducible element is prime.*

Definition (UFD)**.** A Unique Factorization Domain is a commutative unital ring R with the following two properties for every nonzero $r \in R$:

UFD

1. $r = r_1 \cdot r_n$ where r_1 through r_n are irreducible;
2. this finite product is unique, so if $r = r_1 \cdots r_n$ and $r = s_1 \cdots s_m$ then $n = m$ and $r_i = u_i s_i$ for some unit $u_i \in R^\times$.

Theorem 2.6. *Every PID is a UFD.*

Corollary 2.7. *$F[x]$ is a UFD. Equivalently, if $f \in F[x]$ is nonzero then $f = c \cdot f_1 \cdot f_2 \cdots f_n$ where $c \in F^\times$ and f_i are monic irreducible polynomials, and this decomposition is unique.*

Problem 2.1. Given a polynomial $f \in F[x]$, how do we check if f is irreducible?

2.2 Roots and Irreducibility

Definition. If f is a nonzero element of $F[x]$ then $a \in F$ is a root of f if $f(a) = 0$. We can use the division algorithm to write f as $g \cdot (x - a) + r$ where $r = 0$ or $\partial(r) \leq \partial(x - a) = 1$, so r is a constant.

Corollary 2.8. *An element $a \in F$ is a root of f if and only if we can write it as $f = g \cdot (x - a)$.*

Corollary 2.9. *If $f \in F[x]$ and $\partial(f) = n > 0$ then f has at most n roots.*

Proof. Either by induction using $f = g \cdot (x-a) = h \cdot (x-b) \cdot (x-a) = \cdots$ or we use the fact that $F[x]$ is a UFD, so we write f as $f_1 \cdots f_m$ and we know that $m \leq n$ and if any f_i is nonlinear then it has no roots. ■

Example 2.2 (Polynomials with no roots)**.**
Consider $f : x \mapsto x^2 + 1$ in $\mathbf{R}[x]$.
Consdier $f : x \mapsto x^2 - 2$ in $\mathbf{Q}[x]$.
Consider $f : x \mapsto x^2 + x + 1$ in $\mathbf{F}_2[x]$.

Proposition 2.10. *If $f \in F[x]$ is irreducible of degree greater than or equal to 2 then f has no roots in F.*

Proof. $F[x]$ is a unique factorization domain, so we can't write it as a product of anything of a smaller degree, which we showed is the same as writing it as a $(x-r)\cdot g$ in some way. ■

Proposition 2.11. *If $f \in F[x]$ is a polynomial degree at most 3 and f has no roots then f is irreducible.*

Proof. Unique Factorization! Assume that f is reducible and $\partial(f) \leq 3$. Then $f = c \cdot f_1 f_2$ where f_1 and f_2 are nonconstant. If $\partial(f) \leq 3$ then $\partial(cf_1f_2) = \partial(f_1) + \partial(f_2) \leq 3$. Since $\partial(f_i) > 0$ then $\partial(f_1) = \partial(f_2) = 1$, which means that we found linear polynomials and therefore roots. ■

Example 2.3 (Warning)**.** Be careful with the above! Consider $(x^2+1)^2 \in \mathbf{R}[x]$. This has no roots but is irreducible.

Example 2.4 (Warning)**.** The fact that the number of roots is at most the degree fails if we don't work in a field. Consider $f(x) = x^2 - 1 \in \mathbf{Z}/8\mathbf{Z}[x]$. This has degree 2 but all odd numbers less than eight are roots.

Theorem 2.12 (Fundamental Theorem of Arithmetic)**.** *Any nonconstant $f \in \mathbf{C}[x]$ has a root. Then any irreducible polynomial $f \in \mathbf{C}[x]$ is linear.*

Problem 2.2 (Proving Irreducibility).

(a) If $\partial f \leq 3$ then it is irreducbile if it has no roots.

(b)

Theorem 2.13. *Assume $f(x) \in \mathbf{Z}[x]$, and assume that p is a prime such that p doesn't divide a_n and $\bar{f}(x) = \bar{a}_n x^n$ is irreducible, then f is irreducible over $\mathbf{Z}[x]$. This is a reduction ring homomorphism $\mathbf{Z}[x] \to \mathbf{F}_p[x]$.*

3 Tuesday, January 22

Recall that there is a ring homomorphism from $\mathbf{Z}[x]$ to $\mathbf{F}_p[x]$ which is reduction modulo p of the coefficients. There is subtlety when we talk about irreducibility in $\mathbf{Z}[x]$; consider that $2x - 2 = 2 \cdot (x-1)$ is not irreducible as an element of the ring $\mathbf{Z}[x]$, but it is irreducible as a polynomial in a polynomial ring over a field in the sense that we cannot factor it as $g \cdot h$ where $\partial g, \partial h > 0$. This is why we care about nonconstant factors. This discrepancy occurs when we have 2 appearing everywhere, which seems to present a problem. We need a way to distinguish between these two conflated notions.

Definition (Primitive)**.** A polynomial $f \in \mathbf{Z}[x]$ if its coefficients are *all* relatively prime, so that the ideal $(a_0, \ldots, a_n)$ is simply $\mathbf{Z}$, or equivalently that there exist $b_0, \ldots, b_n \in \mathbf{Z}$ such that $\sum b_i a_i = 1$. *Primitive*

Example 3.1. The polynomial $4x^3 + 6x^2 + 15x + 9$ is primitive while $4x^3 + 6x^2 + 16x + 18$ is not, since every term is divisible by 2.

Proposition 3.1. *A polynomial $f \in \mathbf{Z}[x]$ is primitive if and only if its reduction $\bar{f}$ modulo p is not the zero polynomial for all prime p.*

Lemma 3.2. *Let $f \in \mathbf{Q}[x]$. Then there exists a unique rational $c \in \mathbf{Q}$ and a unique primitive polynomial $f_0 \in \mathbf{Z}[x]$ such that $f = c \cdot f_0$.*

Proof. We first prove the existence, and then the uniqueness. Existence is given by clearing the denominators in a smart way, first be clearing the denominators and then by factoring out the GCD of the remaining integral coefficients. The uniqueness arises from the following. Suppose that $c \cdot f_0 = c' \cdot f_0'$ where $c, c' \in \mathbf{Z}$ and f_0, f_0' are primitive. Then if we write $f_0 = aa_n x^n + \cdots + a_0$ and $f_0' = a_n' x^n + \cdots + a_0'$ and the original polynomial as $f = A_n x^n + \cdots + A_0$, then $\gcd(A_0, \ldots, A_n) = \gcd(ca_0, \ldots, ca_n) = \gcd(c'a_0', \ldots, c'a_n')$. Since the GCD is multiplicative we know that these are $c \cdot \gcd(a_0, \ldots, a_n)$ and $c' \cdot \gcd(a_0', \ldots, a_n')$, and since these polynomials are primitive this GCD is 1, so $c = c'$. ■

Lemma 3.3. *If we start with a polynomial in $\mathbf{Z}[x]$, then the c which we pull out will also be an integer.*

Lemma 3.4. *Let $f, g \in \mathbf{Z}[x]$ be primitive. Then $f \cdot g \in \mathbf{Z}[x]$ is also primitive.*

Proof. If f, g are primitive then $\bar{f}, \bar{g} \in \mathbf{F}_p$ are nonzero for all p. Since $\mathbf{F}_p$ has no zero divisors (integral domain) then we know that $\bar{f} \cdot \bar{g}$ is also nonzero in $\mathbf{F}_p$ for all p. Then $fg \in \mathbf{Z}[x]$ is primitive. ■

Lemma 3.5. *If $f \in \mathbf{Z}[x]$ is primitive and $g \in \mathbf{Z}[x]$ is any polynomial, then if f divides g in $\mathbf{Q}[x]$ then f divides g in $\mathbf{Z}[x]$.*

Example 3.2 (Counter example when not primitive)**.** Consider that $4x$ divides $x(x-1)$ in $\mathbf{Q}[x]$ but not in $\mathbf{Z}[x]$ because $4x$ is not primitive.

Proof. There exists some unique way of writing g as $c \cdot g_0$. Since f divides g in $\mathbf{Q}[x]$ then $g = f \cdot h$ for some $h \in \mathbf{Q}[x]$. Thus $f \cdot h = c \cdot g_0$, and we can write $h = d \cdot h_0$. Then $g = d \cdot f \cdot h_0$, and since f and h_0 are primitive we know that fh_0 is primitive as well. Since this decomosition is unique, this implies that $c = d$ and $g_0 = fh_0$. Then f divides g_0 and g_0 divides g in $\mathbf{Z}[x]$, so f divides g in $\mathbf{Z}[x]$. ■

Lemma 3.6 (Gauss)**.** *Let $f \in \mathbf{Z}[x]$. If f is an irreducible polynomial in $\mathbf{Z}[x]$ then f is irreducible in $\mathbf{Q}[x]$.*

Proof. Assume $f = gh$ in $\mathbf{Q}[x]$ where $\partial g > 0$. Write $f = bf_0$, $g = cg_0$, and $h = dh_0$. Then $bf_0 = gh = cdg_0h_0$. Then g_0h_0 is primitive, so $f_0 = g_0h_0$ and $f = bg_0h_0$. ■

Lemma 3.7 (Eisenstein's Criterion)**.** *Let $f = \sum a_i x^i \in \mathbf{Z}[x]$. Fix a prime p and assume the following:*

1. *p does not divide a_n;*
2. *p divides all a_i where $0 \leq i \leq n-1$; and*
3. *p^2 does not divide a_0.*

Then f is irreducible in $\mathbf{Z}[x]$, and by Gauss' Lemma in $\mathbf{Q}[x]$ as well.

Proof. Proof by contradiction. Assume f has the requisite properties but f is reducible in $\mathbf{Z}[x]$, so $f = gh$. Let $g = \sum_{0 \leq i \leq m} g_i x^i$ and $h = \sum_{0 \leq i \leq \ell} h_i x^i$. Consdier $\bar{f} = \bar{a}_n x^n = \bar{g}\bar{h}$. Recall that $a_n = g_m h_\ell$ and $a_0 = g_0 h_0$. Then p divides g_0 and h_0; then p^2 divides $g_0 h_0 = a_0$ which is a contradiction. ■

Example 3.3. Consider that $x^2 - p$ is irreducible in $\mathbf{Q}[x]$ by Eisenstein. Thus $\sqrt{p}$ is irrational. And just like that, most of ancient greek mathematics is solved.

Example 3.4. Notice that $x^p - 1 = (x-1) \cdot x^{p-1} + x^{p-2} + \cdots + 1 = (x-1)\Phi_p(x)$. This is irreducible by Eisenstein.

Proof. Consider $\Phi_p(x+1)$, so $(x+1)^p - 1 = x \cdot \Phi_p(x+1)$. We can use the binomial theorem to say that

$$(x+1)^p = \sum \binom{p}{i} x^i = x^p + px^{p-1} + \cdots + px + 1.$$

Then

$$\Phi_p(x+1) = x^{p-1} + px^{p-1} + \cdots + p.$$

Recall that p divides $\binom{p}{i}$ for all $1 \leq i \leq p-1$. Then $\Phi_p(x+1)$ is Eisenstein, and so $\Phi_p(x+1)$ is irreducible, and so $\Phi_p(x)$ is irreducible. ■

Problem 3.1 (Challenge, find a better proof than the current one which is terrible)**.** Prove that $x^n + x + 1 \in \mathbf{F}_2[x]$ is irreducible for $n \geq 2$.

4 Thursday, January 24

Definition (Extension)**.** Let k be a field. Then $F \subseteq k$ is a subfield if $F \subseteq k$ is a unital subring and F is a field. We say that k is an extension of F and write k/F. *Extension*

Example 4.1. If k is an extension of F then k has the structure of an F-vector space. The cannonical example for this is thinking of $\mathbf{C}$ as a two-dimensional $\mathbf{R}$-vector space with basis $\{1, i\}$.

Definition. An extension k/F is finite if k is a finite dimensional F-vector space. The degree of k/F, written as $[k : F] = \dim_F k$ is the F dimension of k.

Example 4.2 (Examples of degrees)**.**

1. $\mathbf{C}/\mathbf{R}$ is finite and $[\mathbf{C} : \mathbf{R}] = 2$.
2. $\mathbf{R}/\mathbf{Q}$ is infinite since n-tuples of $\mathbf{Q}$ are countable and $\mathbf{R}$ is uncountable.
3. Let $\mathbf{Q}(i) = \{x + iy \in \mathbf{C} \mid x, y \in \mathbf{Q}\}$. Then $\mathbf{Q}(i)/\mathbf{Q}$ is finite with degree 2.

4.1 Field extensions generated by elements

Let F be a field contained in some field Ω. For $\alpha_1, \ldots, \alpha_n \in \Omega$ we can consider two objects:

1. $F[\alpha_1, \ldots, \alpha_n] \subseteq \Omega$ is a subring
2. $F(\alpha_1, \ldots, \alpha_n) \subseteq \Omega$ is a subfield

We define these equantities in the following way.

$$F[\alpha_1, \ldots, \alpha_n] = \bigcap_{\substack{R \subseteq \Omega \\ F \subseteq R, \alpha_i \in R}} R = \left\{ \sum a_{i_1} \cdots a_{i_n} \alpha_1^{i_1} \cdots \alpha_n^{i_n} \mid a_{i_1, \ldots, i_n} \in F \right\}$$

and

$$F(\alpha_1, \ldots, \alpha_n) = \bigcap_{\substack{k \subseteq \Omega \\ F \subseteq k, \alpha_i \in k}} k = \left\{ \frac{\alpha}{\beta} \mid \alpha, \beta \in F[\alpha_1, \ldots, \alpha_n], \beta \neq 0 \right\}.$$

We say that $F[\alpha_1, \ldots, \alpha_n]$ is the subring of Ω generated by $\alpha_1, \ldots, \alpha_n$ and $F(\alpha_1, \ldots, \alpha_n)$ is the subfield of Ω generated by $\alpha_1, \ldots, \alpha_n$.

Example 4.3. Consider $\mathbf{Q}[i]$ and $\mathbf{Q}(i)$. We say that $\mathbf{Q}[i]$ are rational polynomials in i and $\mathbf{Q}(i)$ are quotients of these polynomials, understanding that even powers of i and odd powers of i to collapse it into rational and imaginary components. These are equal to one another. However, $\mathbf{Q}[\pi] \subset \mathbf{Q}(\pi)$ but they are not equal (since the field extension is not finite as π is not algebraic).

The Laurent series $F((x))$ is important for Complex Analysis and is analogous to the formal power series $R[[x]]$.

Theorem 4.1 (Tower Law)**.** *Let L/k and k/F be field extensions. Then $[L : F] = [L : k] \cdot [k : F]$.*

Proof. If L is a finite dimensional F-vector space then L is a finite dimensional k-vector space since if $z_1, \ldots, z_p$ is an F-basis for L then in turn $\alpha = \sum a_i z_i \in F$ for all $\alpha \in L$ so $z_1, \ldots, z_p$ is a generating set. On the other hand, $k \subseteq L$ is an F-vector space. Assume that $[L : k] = n$ with x_i a k-basis for L and $[k : F] = m$ with y_i and F-basis for k. Then we first show that $\{x_i y_j\}$ is an F-basis of L so $[L : F] = nm$. First, linear independence: assume that $\sum a_{i,j} x_i y_j = 0$ for $a_{i,j} \in F$. Rewrite this as $\sum (\sum a_{i,j} y_i) x_i = 0$, so $\sum a_{i,j} y_i = 0$ so $a_{i,j} = 0$ and the set is linearly independent. Next, we show this generates L over F. Let $\alpha \in L$ be written as $\alpha = \sum \beta_i x_i$ for $\beta_i \in k$. But for each i we have $\beta_i = \sum a_{i,j} y_i$ so $\alpha = \sum (\sum a_{i,j} y_i) x_i = \sum a_{i,j} x_i y_i$, so these generate. Then this is a basis, and the proposition holds. ■

5 Tuesday, January 29

Definition (Algebraic)**.** Let k/F be a field extension and let $\alpha \in k$. Then α is algebraic over F if there exists a nonzero $f \in F[x]$ such that $f(\alpha) = 0$. Otherwise, we say that α is trancendental over F.

Algebraic

- $\sqrt{2} \in \mathbf{R}$ is algebraic over $\mathbf{Q}$ since it satisfies $f(x) = x^2 - 2$;
- $\pi \in \mathbf{R}$ is trancendental over $\mathbf{Q}$.

Definition (Simple Field Extension)**.** Let F be a field. Then k/F is a *simple* field extension if $k = F(\alpha)$ for some single $\alpha \in k$.

Simple Field Extension

Theorem 5.1. *Let F be a field, let Ω/F be a field extension, let $\alpha \in \Omega$, and let $k = F(\alpha)$. Then either*

1. *α is trancendental, in which case k/F is not finite; or*
2. *α is algebraic, in which case k/F has finite degree n, $F[\alpha] = F(\alpha)$, and there exists a unique monic irreducible polynomial $m_\alpha(x) \in F[x]$ of degree n such that $m_\alpha(\alpha) = 0$. This m_α is called the minimal polynomial of α over F.*

Lemma 5.2. *If α is trancendental over F then $k = F(\alpha)$ is infinite over F and $F[\alpha] \equiv F[x]$.*

Lemma 5.3. *The polynomial m_α is the unique monic polynomial of minimal degree which has α as a root; consequently, it is irreducible.*

Proof of 5.3. By the proof of EUCLIDEAN $\implies$ PID (i.e., any element of minimal degree in an ideal of $F[x]$ generates the ideal). Hence $m_\alpha(x)$ generates the idea, and so it is the unique monic element of minimal degree. To show it is irreducible, suppose that $m_\alpha = fg$; then $m_\alpha(\alpha) = f(\alpha)g(\alpha) = 0$. Since K has no zero divisors we know that $f(\alpha) = 0$ or $g(\alpha) = 0$. Assume without a loss of generality that $f(\alpha) = 0$. Assume (to get a contradiction) that $\partial f, \partial g < \partial m_\alpha$. However, if this is the case then we have a polynomial with α as a root with a smaller degree than m_α, which we had already shown to be minimal. This presents a contradiction, and so m_α is irreducible. ∎

Proof of part 1. If α is trancendental then $f(\alpha) \neq 0$ for any $f \in F[x]$. There is a unique F-algebra homomorphism from $F[x] \to k$ such that $x \mapsto \alpha$. Since the kernel of this map is trivial (since nonzero polynomials don't satisfy α) then this F-algebra homomorphism is injective. The image of this homomorphism is precisely $F[\alpha] \subseteq k$. Then by the First Isomorphism Theorem for Rings, we know that $F[x] \equiv F[\alpha]$ since the kernel is trivial. But $F[\alpha]$ is an F-vector space with infinite F-dimension. Hence

$F(\alpha)$ is also of inifinite dimension since $F[\alpha] \subset F(\alpha)$ is an F-subspace. Then the degree of $F(\alpha)$ over F is infinite. ■

Proof of part 2. Since α is alegebraic, we know that the homomorphism is not injective. Then its kernel is a nontrivial ideal $I \subseteq F[x]$, so by PID-ness $I = (g(x))$ for some nonzero $g \in F[x]$. We can call this polynomial $g = m_\alpha$. ■

6 Thursday, January 31

Recall from last lecture: We have a field $F \subseteq \Omega$ and some $\alpha \in \Omega$ with an evaluation homomoprhism $F[x] \to \Omega$ where $x \mapsto \alpha$ and the image is $F[\alpha]$. Then either this is injective, which means that α is trancendental, or we have a nontrivial kernel equal to $(m_\alpha(x)) \subseteq F[x]$ where $m_\alpha(x)$ is the minimal polynomial of α over F.

Recall also from MATH 350 that if R is a PID but not a field and $I \subseteq R$ is a prime ideal then $I \subseteq R$ is a maximal ideal.

Corollary 6.1. *If α is algebraic over F then $F[x]/(m_\alpha(x))$ is a field which is isomorphic to $F[\alpha]$ by the first isomorphism theorem.*

Proof. Recall that the minimal polynomial is irreducible, and in a PID irreducibility implies that it is prime. Then (m_α) is a prime ideal and so maximal. Then $F[x]/(m_\alpha)$ is a field. ■

Corollary 6.2. *If α is algebraic over F then $F[\alpha] = F(\alpha)$.*

Proof. By definition $F[\alpha] \subseteq F(\alpha)$. Since $F[\alpha]$ is a field containing F, α and $F(\alpha)$ is the smallest extension of F containing α then $F(\alpha) \subseteq F[\alpha]$, and so they are equal by dual containment. ■

Theorem 6.3. *Let $f(X) \in F[x]$ be irreducible of degree n. Then $F[x]/(f)$ is a field extension of F of degree n with an F-basis $\{\bar{1}, \bar{x}, \bar{x}^2, \dots, \bar{x}^{n-1}\}$ where $\bar{x}$ is the coset in $F[x]/(f)$ represented by x.*

Proof. By the corollaries, $K = F[x]/(f)$ is a field extension of F. Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n$. We claim then taht $1, \bar{x}, \dots, \bar{x}^{n-1}$ is generates K over F. We know that K is generated by the infinite set $\bar{1}, \bar{x}, \bar{x}^2, \dots$. However we see that $\bar{x}^n = 1\frac{1}{a_n}(a_0 + a_1\bar{x} + \cdots + a_{n-1}\bar{x}^{n-1})$, and so on for $\bar{x}^k$ for $k \geq n$. All of these expressions are linear combinations of $\bar{1}, \bar{x}, \dots, \bar{x}^{n-1}$. Then we must show that these are all linearly independent. Suppose that

$$b + b_1\bar{x} + \cdots + b_{n-1}\bar{x}^{n-1} = 0.$$

Notice that $\bar{x} \in K$ satisfies $f(\bar{x}) = 0$ and f is irreducible ofer F. Then $\frac{1}{a_n} f(x)$ is the minimal polynomial of $\bar{x} \in K$. Then no polynomial of smaller degree can have $\bar{x}$ as a root, yet we just found $\star$ to have $\bar{x}$ as a root, and so $b_i = 0$ for all i and this set is linearly independent. ■

Corollary 6.4. *Let $\alpha, \beta \in \Omega$ have the same minimal polynomial over F. Then $F(\alpha) \equiv F(\beta)$.*

Definition. $F(\alpha_1, \ldots, \alpha_n)$ is a field extension of F which is finitely generated.

Theorem 6.5. *Let F be a field.*

1. *Any finite extension k/F is algebraic, where every elemetn $\alpha \in k$ is algebraic over F.*

2. *Any finitely-generated and algebraic extension k/F is finite.*

7 Tuesday, February 5

7.1 Ruler and Compass Construction

Euclid had this book which tried to lay the foundations for geometry. Among these are *constructions.*

1. You have a set $S, \mathcal{P} \subseteq \mathbf{C}$ which contain 0 and 1.

2. Given any two points p, q in S, you can draw a line $\overline{PQ}$ through p and q.

3. Given any two points p, q in S you can draw the circle $C_p(q)$ centered at p going through q.

4. Any intersections of lines or circles which can be drawn are now points in $\mathcal{P}$.

We call $\mathcal{P} \subseteq \mathbf{C}$ the set of constructable numbers which contains $0, 1$ and is closed under this method of constructions. We can also create this idea algorithmicly. We proceed with induction for $n \geq 0$. Let $\mathcal{P}_0 = \{0, 1\}$ and let $\mathcal{L}_0 = \mathcal{C}_0 = \emptyset$. Let $\mathcal{L}_{n+1} = \{\ell_{p,q} \mid p, q \in \mathcal{P}_n\}$ and let $\mathcal{C}_{n+1} = \{C_p(q) \mid p, q \in \mathcal{P}_n\}$. Then

$$\mathcal{P}_{n+1} = \{z \in \mathbf{C} \mid z \in L \cap L', C \cap L, C \cap C', L, L' \in \mathcal{L}_{n+1}, C, C' \in \mathcal{C}_{n+1}\}.$$

Hence $\mathcal{P}_0 \subseteq \mathcal{P}_1 \subseteq \cdots \subseteq \mathcal{P}$, and each $\mathcal{P}_n$ are finite. Then $\bigcup_{n \geq 0} \mathcal{P}_n = \varinjlim \mathcal{P}_n = \mathcal{P}$. Then $\mathcal{P}$ is countable.

Theorem 7.1. *The set $\mathcal{P} \subset \mathbf{C}$ is a field called Pythagorean closure of $\mathbf{Q}$ in $\mathbf{Q}$.*

7.2 Some Basic Constructions

1. Given a 'line segment' $\overline{PQ}$ we can bisect it by drawing the circles $C_p(q)$ and $C_q(p)$ and then drawing the line connecting the intersections of these circles.

2. Given a line ℓ and a $p \in \ell$ we can draw the perpendicular line to ℓ at p. Draw a circle $C_p(q)$ where q is any other point on ℓ. Then draw two circles of twice the radius centered at the intersections of the smaller circle with ℓ, and then connect their intersections.

3. Give a line ℓ and a point $p \notin \ell$ we can draw the parallel line to ℓ through p. Draw a circle centered at p intersecting ℓ. Draw the perpendicular bisector of ℓ through p.

8 Wednesday, 7 January

More constructions.

9 Tuesday, 12 January

Recall that $\mathfrak{p} \subseteq \mathbf{C}$ is the subfield of constructible numbers, and $\mathbf{Q}^{\text{py}} \subseteq \mathbf{Q}$ is the Pythagorean closure of the rationals. We had a theorem that these were equal to one another. A corollary to this is the fact that $\alpha \in \mathfrak{p}$ if and only if there exists a tower of fields of relative degree two ending at $\mathbf{Q}(\alpha)$, which tells us that $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 2^n$. This proves that we cannot double the cube since $[\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}] = 3$.

9.1 Squaring the Circle

There is also the problem of squaring the circle, which is also impossible since if a circle has area π then the sides of the square would need length $\sqrt{\pi}$, which is not algebraic in $\mathbf{Q}$. This implicitly assumes that all constructible numbers are algebraic, which isn't necessarily a trivial observation. However, part of proving that $\mathfrak{p}$ is a field is showing that $\mathfrak{p}/Q$ is algebraic.

9.2 Trisecting an Arbitrary Angle

The general statement of this problem is on the homework. Consider $\theta = 2\pi/3$. Then $\theta/3 = 2\pi/9$. The intersection of θ with the unit circle is ω and the intersection with $\theta/3$ with the unit circle is ζ_9. Then the constructibility $\theta/3$ is then equivalent to the constructibility of ζ_9. Since the minimal polynomial of $\cos(\zeta_9)$ has degree three, it is not constructible.

Lemma 9.1. *The angle $2\pi/n$ is constructible if and only if ζ_n is constructible if and only if $\cos(2\pi/n)$ and $\sin(2\pi/n)$ are constructible.*

9.3 Splitting Fields

Let $F \subseteq \Omega$ be a field and let $f(x) \in F[x]$ have degree n. We say that f splits in Ω if $f(x) = a\prod(x - \alpha_i)$ for $\alpha_i \in \Omega$, so it separates into linear factors.

Example 9.1. Consider $f(x) = x^3 - 2 \in \mathbf{Q}$. We know that $\sqrt[3]{2}$ is a real root. How does $f(x)$ split in $\mathbf{Q}\big(\sqrt[3]{2}\big)$. Since it has a root, we know it factors as $f = (x - \sqrt[3]{2})g(x)$ where $g \in \mathbf{Q}\big(\sqrt[3]{2}\big)[x]$ has degree two. We can calculate what g is through polynomial division to get that

$$f(x) = \left(x - \sqrt[3]{2}\right)\left(x^2 + \sqrt[3]{2}x + \sqrt[3]{2}^2\right).$$

We can check the discriminant is negative to see that the remaining quadratic has complex roots, and so cannot split further over $\mathbf{Q}\big(\sqrt[3]{2}\big)$.

Definition (Splitting field)**.** A splitting field for $f(x) \in F[x]$ is an extension E/F such that *Splitting field*

- $f(x)$ splits in E, so $f = a\prod(x-\alpha_i)$
- $E = F(\alpha_1, \ldots, \alpha_n)$.

In this way, it is kinda like the "minimal field" over which f splits.

Theorem 9.2. *Let $f \in F[x]$. Then a splitting field E/F for f exists, and moreover if $\deg(f) = n$ then $[E : F] \leq n!$.*

Example 9.2. Recall the Cyclotomic polynomial $\Phi_p(x) = (x^p - 1)/(x-1)$ for prime p. Any p^{th} root of 1 is a root since $\Phi_p(\zeta_p) = (\zeta_p^p - 1)/(\zeta_p - 1) = 0$. But ζ_p^k is also a root, and there are $p-1$ of them, which is the degree of $\Phi_p(x)$. So in fact $\Phi_p(x)$ splits over $\mathbf{Q}(\zeta_p)$.

Proof of the existence of a finite splitting field. We can find the splitting field by adjoining all the roots to $\mathbf{Q}$. Then its finitely generated and algebraic, so it is finite. ■

Proof of the bound on the degree. Just divide the polynomial by the one root we do have to get a polynomial of degree $n-1$. Then repeat the procedure until we get linear terms. Then we have a tower where the relative degree of the i^{th} is $n-i$, and so the degree of the full extension is bounded by $n \cdot (n-1) \cdots 1 = n!$. ■

Theorem 9.3. *Splitting fields are unique up to an F-isomorphism.*

Theorem 9.4. *Let $f \in F[x]$ be a monic polynomial. Let E/F be generated by some subset of the roots of f. Let Ω/F be a field extension where f splits. Then*

(a) *There exist F-homomorphisms $\phi_i : E \to \Omega$, and the number of distinct ϕ_i is at most $[E : F]$ with equality if f has distinct roots;*

(b) *If E and Ω are splitting fields then they are isomorphic.*

10 Thursday, 14 February ♡

10.1 Splitting Fields

Splitting fields are unique up to F-isomorphism.

Extension Fields Let F be a field, and let K/F, Ω/F be extensions of F. A map $\phi\colon K \to \Omega$ if ϕ is an F-homomorphism if it is a ring homomorphism which preserves F. This means that ϕ is an F-linear map of vectorspaces. Let $\operatorname{Hom}_F(K, \Omega)$ be the set of F-homomorphisms. Since F-homomorphisms are injectives, we refer to them as embeddings or F-embeddings.

Example 10.1 (Examples of F-homomorphisms)**.**

- Complex conjugation $\sigma\colon \mathbf{C} \to \mathbf{C}$ is an $\mathbf{R}$-homomorphism which sends i to $-i$. In fact, $\operatorname{Hom}_{\mathbf{R}}(\mathbf{C}, \mathbf{C}) = \{\mathrm{id}, \sigma\}$.

Theorem 10.1 (Extension Theorem)**.** *Let $F(\alpha)$ be a simple extension of F, and let Ω/F be an extension of F.*

(a) *Assume that α is trancendental over F. Then for every F-homomorphism ϕ between $F(\alpha)$ and Ω, the image $\phi(\alpha)$ is trancendental over F and there is a bijection between $\operatorname{Hom}_F(F(\alpha), \Omega)$ and the set of all trancendental elements of Ω given by $\alpha \mapsto \phi(\alpha)$.*

(b) *Assume that α is algebraic over F and let $f \in F[x]$ be its minimal polynomial. Then for every F-homomorphism ϕ between $F(\alpha)$ and Ω, the image $\phi(\alpha)$ is a root of f and there is a bijection between $\operatorname{Hom}_F(F(\alpha), \Omega)$ and the set of roots of f in Ω. In particular, the size of $\operatorname{Hom}_F(F(\alpha), \Omega)$ is equal the number of distinct roots of f in Ω.*

Example 10.2.

- Consider $\mathbf{Q}(\sqrt[3]{2})$ whose minimal polynomial is $x^3 - 2$. The size of $\operatorname{Hom}_{\mathbf{Q}}(\mathbf{Q}(\sqrt[3]{2}), \mathbf{R})$ is 1 since $x^3 - 2$ has only one real root. The lone element is the identity map id.
- Consider $\operatorname{Hom}_{\mathbf{Q}}(\mathbf{Q}(\sqrt[3]{2}), \mathbf{C})$. We know that this has size 3 since there are three complex roots of $x^3 - 2$. We know that $\mathrm{id} \in \operatorname{Hom}_{\mathbf{Q}}(\mathbf{Q}(\sqrt[3]{2}), \mathbf{C})$, but what are the other two. Call them ϕ_1 and ϕ_2, where $\phi_1\colon \sqrt[3]{2} \mapsto \omega \sqrt[3]{2}$ and $\phi_2\colon \sqrt[3]{2} \mapsto \bar{\omega}^2 \sqrt[3]{2}$.

Proof of Extension Theorem.

(a) Assume that α is trancendental over F. Recall that $F[\alpha] \simeq F[x]$. Given any $\beta \in \Omega$ which is trancendental over F, we know that there exists a unique F-algebra homomorphism $\phi\colon F[x] \to \Omega$ given by $x \mapsto \beta$. Since β is trancendental, we know ϕ to be injective. Since it is injective, it extends uniquely to a homomorphism $\phi\colon F(x) \to \Omega$, and so $\tilde{\phi}\colon F(\alpha) \simeq F(x) \overset{\phi}{\hookrightarrow} \Omega$ by $\alpha \mapsto x \mapsto \beta$. So we've found an F-homomorphism $\tilde{\phi}\colon F(\alpha) \to \Omega$, which means that the map is both injective and surjective and so it's bijective.

(b) Assume that α is algebraic. Note that if $f = \sum a_i x^i$ then consider $0 = f(\alpha)$, and so $\phi(0) = 0 = \phi\left(\sum a_i \alpha^i\right)$. Since ϕ is an F-homomorphism it breaks on addition and multiplication and preserves a_i, so $0 = \sum a_i \phi(\alpha)^i$. We can extend this into the statement
$$\phi(f(\beta)) = f(\phi(\beta))$$
for any β. Then $\phi(\alpha)$ is a root of f. As before, we have an injective map between $\mathrm{Hom}_F(F(\alpha), \Omega)$ to the roots of f in Ω since any F-hom is injective, and so $\phi\colon F(\alpha) \to \Omega$ is uniquely determined by where α is sent. To show surjectivity, let $\beta \in \Omega$ be a root of f. Now, as before, we must construct an F-homomorphism which takes α to β. Remember that $F(\alpha) \simeq F[x]/(f(x))$. Also, look at the map $F[x] \to \Omega$ where $x \mapsto \beta$. Since β is a root of the minimal polynomail, this map does have a kernel, whose elements are generated by $(f(x))$. Then by the First Isomorphism Theorem, we know that $F[x]/(f(x)) \simeq F(\beta) \subseteq \Omega$, and so it total we have
$$\tilde{\phi}\colon F(\alpha) \simeq F[x]/(f(x)) \simeq F(\beta) \subseteq \Omega,$$
and the composition $\tilde{\phi}$ of F-homomoprhisms sends α to β. ■

Theorem 10.2 (Extension Theorem′ (Algebraic Case))**.** *Let ψ be some embedding from F into Ω (maybe not an F-homomorphism). We say that $\phi\colon F(\alpha) \to \Omega$ extends ψ if ϕ is a ring homomorphism and $\phi(c) = \psi(c)$ for all $c \in F$, and the following diagram commutes.*

$$\begin{array}{ccc} F(\alpha) & \xrightarrow{\phi} & \Omega \\ \uparrow & & \| \\ F & \xrightarrow{\psi} & \Omega \end{array}$$

Corollary 10.3. *Any F-homomorphism is an extension of the identity map* $\mathrm{id}(x)$.

Proposition 10.4. *Let $f \in F[x]$ be monic, and let E/F be an extension generated by some subset of the roots of f; i.e., $E = F(\alpha_1, \ldots, \alpha_n)$ where $f(\alpha_i) = 0$ for all i. Let Ω be an extension of F where f splits.*

(a) *There exist F-homomorphisms ϕ_i from E to Ω, and $|\phi_i| \leq [E : F]$ with equality when f has distinct roots in Ω.*

(b) *If both E and Ω are splitting fields of f then there exists an F-isomorphism from E to Ω.*

Proof. Some observations:

1. If α is a root of f in Ω and $m(x) \in F[x]$ is the minimal polynomial of α over F, then in fact m divides f, since the minimal polynomial generates all polynomials which have α as a root.

2. If you have some subextension between F and Ω, like $F \subseteq L \subseteq \Omega$ where $f = g \cdot h$ in $L[x]$, then the roots of g in Ω are among the roots of f in Ω, and so g must split in Ω as well.

We'll use these several times.

(a) First write E as $F(\alpha_1, \ldots, \alpha_n)$. Let $f_1 \in F[x]$ be the minimal polynomial of α_1, and so by Observation 1 we know that $f_1 \mid f$, and f_1 splits in Ω by Observation 2, and the roots of f_1 are distinct if f has distinct roots. By the extension theorem, there exists an F-homomoprhism $\phi_1 \colon F(\alpha_1) \to \Omega$, and the number of such ϕ_1 is bounded by the degree of f_1 which is $[F(\alpha) : F]$. Since each subsequent extension is simple over the previous, we can construct the following diagram of extensions.

$$\begin{tikzcd}
E \arrow[r, "\phi"] \arrow[d, dotted, no head] & \Omega \\
F(\alpha_1, \alpha_2) \arrow[ur, "\phi_2"] \arrow[d, no head] & \\
F(\alpha) \arrow[uur, "\phi_1"] \arrow[d, no head] & \\
F &
\end{tikzcd}$$

■

11 Thursday, 21 February 2019

"You are right to be skeptical of this calculus business"

Asher

Recall our proposition:

Proposition 11.1. *Let $f \in F[x]$ and let E/F be an extension generated by some subset of the roots of f. Suppose that Ω/F is the splitting field of f. Then $1 \le \# \operatorname{Hom}_F(E, \Omega) \le [E : F]$ with upper-bound equality when f has all distinct roots.*

Corollary 11.2. *If E, E' are splitting fields of f then $E \simeq E'$.*

Proof. Let $E = \Omega$ as in the above proposition, and exhibit an F-homomorphism. Then let $E' = \Omega$, and do the same. Since F-homs are injective, and we have two finite dimensional vector-spaces with injective homs between them, then they are isomorphic. ■

Corollary 11.3. *If E/F is any finite extension and L/F is any extension then $\# \operatorname{Hom}_F(E, L) \le [E : F]$ and there always exists an extension Ω/L such that $\operatorname{Hom}_F(E, \Omega) \ne \varnothing$.*

11.1 Multiple Roots

Let $f \in F[x]$ be a polynomial, and let Ω be a field in which f splits, and let $\alpha \in \Omega$ is a root of f.

> **Definition** (Multiple, Simple Roots; Seperable)**.** We say that α is multiple root of f if and only if $(x-\alpha)^k$ divides f over Ω for multiplicity $k > 1$. Otherwise, we say that α is a simple root. The polynomial f is seperable if every root is simple.

Multiple, Simple Roots; Seperable

Over $\mathbf{C}$, we can test for multiple roots. Suppose that $f(x) = (x-\alpha)^2 g(x)$. Consider the derivative of f, which is

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

Notice that we can factor out a term of $(x-\alpha)$. More generally, if f has a root of multiplicity at least m, then f' has the same root with multiplicity at least $m-1$. This gives us the formula

$$\operatorname{mult}_\alpha f = \max\{i < \deg f \mid f^{(i)}(\alpha) = 0\}.$$

This implies that $(x-\alpha)$ divides $\gcd(f, f')$.

11.2 The Derivative

For any polynomial $f = \sum a_i x^i$, define $f' = \sum i a_i x^{i-1}$. This has some nice properties:

- $d/dx \colon F[x] \to F[x]$ is F-linear;
- $d/dx(a) = 0$ for constant a;
- The Chain Rule;
- The Product Rule;

Proof. Induction. ∎

Proposition 11.4. *Let $f \in F[x]$. Then f is seperable if and only if f and f' are relatively prime.*

Proof. "$\implies$" Let f be seperable, and let Ω be a field where f splits, and let $\alpha \in \Omega$ be a root of f. Then α is simple if and only if $f(x) = (x - \alpha)h(x)$ and $h(\alpha) \neq 0$. Consider $f'(x) = h(x) + (x - \alpha)h'(x)$ by the chain/product rules, and so $f'(\alpha) \neq 0$. Thus no root of f is a root of f', and hence they share no common factors and so are relatively prime in F.

"*impliedby*" Proof by contrapositive. Assume that f is not seperable, and let α be a multiple root. Hence $f(x) = (x - \alpha)^2 g(x)$ over Ω. Then $f' = 2(x - \alpha)g(x) + (x - \alpha)^2 g'(x)$, and so $f'(\alpha) = 0$. Then f and f' have a common root, and so $m_\alpha(x)$ divides both f and f' over F. Thus their GCD is not 1, and so they are not relatively prime. ∎

Exercise 11.1. Let $D \colon F[x] \to F[x]$ be an F-linear map satisfying the product rule and $D(x) = 1$. Prove that D is exactly the derivative. (Hint: Try Induction.)

Definition (Seperable Extension)**.** An algebraic etension K/F is called seperable if every element $\alpha \in K$ satisfies a seperable polynomial over F. Equivalently, the minimal polynomial over F of every $\alpha \in K$ is seperable.

Seperable Extension

Proposition 11.5. *Some nice facts:*

1. *Let $f \in F$ be irreducible. Then f is seperable if and only if the derivative doesn't vanish.*

2. *If* $\operatorname{char} F = 0$ *(so* $\mathbf{Q} \subseteq F$*) then every irreducible polynomial is seperable.*
3. *If* $\operatorname{char} F = p$ *(so* $p = 0 \in F$*) then* f *is not seperable if and only if* $f(x)$ *is a polynomial in* x^p*, so* $f(x) = g(x^p)$*.*

12 No Notes

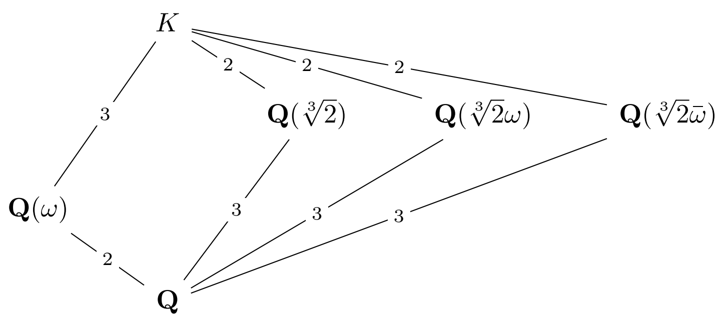
13 No Notes

14 Tuesday, 5 March 2019

"Let's do more boring stuff."

Asher

Recall splitting fields. Let K be the splitting field of $x^3 - 2$. We showed that $K = \mathbf{Q}(\sqrt[3]{2}, \omega)$ with the following structure.



We know that $\#\operatorname{Aut}_{\mathbf{Q}}(K) \leq 6$ since any $\phi\colon K \to K$ is determined by the three choices for $\phi(\sqrt[3]{2})$ and the two choices for $\phi(\omega)$.

Fact: $K/\mathbf{Q}(\sqrt[3]{2}\omega^2)$ is a degree two extension.

Consider $\sigma_i\colon K \to K$ where $\sigma\colon \omega \mapsto \bar{\omega}$. Then we get the following possible automorphisms:

$$\begin{aligned}
\sigma_0\colon &= \sqrt[3]{2} \mapsto \sqrt[3]{2}, \omega \mapsto \bar{\omega} \\
\sigma_1\colon &= \sqrt[3]{2}\omega \mapsto \sqrt[3]{2}\omega, \omega \mapsto \bar{\omega} \\
\sigma_2\colon &= \sqrt[3]{2}\bar{\omega} \mapsto \sqrt[3]{2}\bar{\omega}, \omega \mapsto \bar{\omega}
\end{aligned}$$

Now consider

$$\begin{aligned}
\rho = \sigma_2\sigma_0\colon K &\longrightarrow K \\
\sqrt[3]{2} &\mapsto \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega \\
\omega &\mapsto \bar{\omega} \mapsto \omega
\end{aligned}$$

and

$$\begin{aligned}
\tau = \sigma_1\sigma_0\colon K &\longrightarrow K \\
\sqrt[3]{2} &\mapsto \sqrt[3]{2} \mapsto \sqrt[3]{2}\bar{\omega} \\
\omega &\mapsto \bar{\omega} \mapsto \omega
\end{aligned}$$

Then we've found six automorphisms $\{\mathrm{id}_K, \sigma_0, \sigma_1, \sigma_2, \rho, \tau\}$. Since our upper bound was six, we've found all possible automorphisms of $\mathrm{Aut}_{\mathbf{Q}}(K)$. Furthermore, note that every σ_i has order 2. Now we wan't to find some relations. Note that $\rho^2 = \tau$ and $\rho^3 = \mathrm{id}_K$. From this, we can tell that $\mathrm{Aut}_{\mathbf{Q}}(K) \simeq D_6 \simeq S_3$.

Remember that $\mathrm{Aut}_{\mathbf{Q}}(K)$ permutes the roots of $x^3 - 2$. This is a general phenomenon. If f is a polynomial over F and E is the splitting field of f over F then $\mathrm{Gal}(f) = \mathrm{Aut}_F(E)$. Assume f is seperable of degree n with roots $\{\alpha_i\}$ and so $E = F(\{\alpha_i\})$. Then $\mathrm{Gal}(f)$ acts on $\{\alpha_i\}$ and $\mathrm{Gal}(f)$ acts on E by F-automorphism. The action of $\mathrm{Gal}(f)$ on $\{\alpha_i\}$ is faithful, so the kernel of the action is trivial.

Proof. If $\sigma \in \mathrm{Gal}(f)$ fixes all α_i then $\sigma = \mathrm{id}$ on E since α_i generate E over F. ■

Recall if a group G acts on a set X of order h then there is an induced permutaiton representation

$$\rho \colon G \mapsto S_X = \mathrm{Bij}(x) \simeq S_n : g \mapsto (x \mapsto g \cdot x),$$

and so ρ is a homomorphism of groups. This ρ is injective if and only if G acts faithfully on X.

Corollary 14.1. *If f is seperable of degree n over F then $\mathrm{Gal}(f)$ is isomorphic to a subgroup of S_n. We will soon prove that $[E : F] = \#\,\mathrm{Gal}(f)$, which gives immediately that $[E : F] \mid n!$ by Lagrange. Given any K/F finite, we'll soon prove that $\#\,\mathrm{Aut}_F K \leq [K : F]$.*

Definition (Galois Extension)**.** A finite extension K/F is Galois if *Galois Extension*

$$\#\,\mathrm{Aut}_F K = [K : F].$$

We'll soon see that the splitting field of any seperable polynomial is Galois.

Definition. Define the following set

$$\mathrm{Hom}_{F\text{-vs}}(K, \Omega) = \{\varphi \colon K \to \Omega \mid \varphi \text{ is } F\text{-linear}\}.$$

These aren't the field embeddings we've been dealing with. We require that $\phi(\lambda a) = \lambda\phi(a)$ and $\phi(a+b) = \phi(a)+\phi(b)$ but nothing more. THese are basically just matrices; if $[K : F] = n$ and $[\Omega : F] = m$ then $\mathrm{Hom}_{F\text{-vs}} \simeq \mathrm{Mat}_{m\times n}(F)$. These aren't super nice but are very easy to describe. In particular, we know that it is an F-vector space of dimension nm. Something actually interesting and non-obvious about this is that it is also an Ω-vector space.

15 Thursday 7 March 2019

Recall that a Galois extension K/F is one whose automorphism group has order equal to the degree of K/F. We also know that if f splits in K that $\mathrm{Gal}(f) = \mathrm{Gal}(K/F)$.

15.1 Galois Correspondence

Let K/F be a finite Galois extension and let $H \leq G = \mathrm{Gal}(K/F)$ be a subgroup of the Galois group of this extension.

Definition (Fixed Field)**.** The fixed field $K^H = \{\alpha \in K \mid \sigma(\alpha) = \alpha \, \forall \sigma \in H\}$. *Fixed Field*

Claim 15.1 — We have a tower of extensions $K/K^H/F$.

Proof. Let $\alpha, \beta \in K^H \subseteq K$. We konw that $\sigma(\alpha) = \alpha$ and $\sigma(\beta) = \beta$ for all $\sigma \in H$. Then $\sigma(\alpha+\beta) = \sigma(\alpha) + \sigma(\beta) = \alpha + \beta$ and $\sigma(\alpha \cdot \beta) = \sigma(\alpha) \cdot \sigma(\beta) = \alpha \cdot \beta$, so $\alpha + \beta$ and $\alpha\beta$ are in K^H. Furthermore, we know that $\alpha\alpha^{-1} = \sigma(\alpha)\sigma(\alpha^{-1}) = 1$, and so $\alpha^{-1} \in K$. Finally, since σ is an F-automorphism then for any $\lambda \in F$ we know that $\sigma(\lambda) = \lambda$, and so K^H is a field. ■

Claim 15.2 — Given a tower $K/L/F$, there exists a subgroup of $\mathrm{Gal}(K/F)$ which fixes L.

Proof. Notes that $\mathrm{Aut}_L K \subseteq \mathrm{Aut}_F K = \mathrm{Gal}(K/F)$. Then simply define H to be the subset of $\mathrm{Gal}(K/F)$ which does fix L, and by similar logic about compositions it will be a subgroup. Thus there is a one-to-one correspondence between subgroups of $\mathrm{Gal}(K/F)$ and subextensions of K/F. ■

$$\left\{\begin{array}{c} K \\ | \\ L \\ | \\ F \end{array}\right\} \qquad \begin{array}{ccc} L & \longrightarrow & \mathrm{Aut}_L K \\ & & \\ K^H & \longleftarrow & H \end{array} \qquad \left\{\begin{array}{c} I \\ | \\ H \\ | \\ G \end{array}\right\}$$

Let's see how this works. We'll proceed through $K/L/F \rightsquigarrow H = \mathrm{Aut}_L K \rightsquigarrow K^H$.

Claim 15.3 — $L \subseteq K^{\mathrm{Aut}_L K}$.

Proof. This just sorta falls out from the definition of what each thing is, since L is obviously fixed by every single element of the automorphism group which fixes L. ■

Theorem 15.1. *These fields are equal:* $L = K^{\operatorname{Aut}_L K}$.

Now let's look at $H \le G \rightsquigarrow K/K^H/F \rightsquigarrow \operatorname{Aut}_{K^H} K$.

Claim 15.4 — $H \le \operatorname{Aut}_{K^H} K$.

Proof. Again, just look at the definitions. ∎

Theorem 15.2. *These groups are equal:* $H = \operatorname{Aut}_{K^H} K$.

Warning 15.1 — Given $K/L/F$, we could consider instead the automorphism group $\operatorname{Aut}_L F$ (instead of $\operatorname{Aut}_L K$). However, this is not a subgroup of $\operatorname{Aut}_F K$.

Example 15.1. Consider the extension $\mathbf{Q}(\sqrt[4]{2})$. There is a very nice extension $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt{2}) \subseteq \mathbf{Q}(\sqrt[4]{2})$. Furthermore, we know that $\mathbf{Q}(\sqrt{2})$ is Galois with a Galois group of $\{\mathrm{id}_{\mathbf{Q}}, \sigma\}$, and $\mathbf{Q}(\sqrt[4]{2})$ is Galois *over* $\mathbf{Q}(\sqrt{2})$ with Galois group $\{1, \tau\}$ where $\tau(\sqrt[4]{2}) = -\sqrt[4]{2}$ and this group fixed $\mathbf{Q}(\sqrt{2})$. However, $\operatorname{Aut}_{\mathbf{Q}} \mathbf{Q}(\sqrt[4]{2}) = \{1, \tau\}$ as well, so there is no way to think of σ as an automorphism of $\mathbf{Q}(\sqrt[4]{2})$.

Question 15.1 — How does this behave in towers?

$$\left\{\begin{array}{c} K \\ | \\ L_1 \\ | \\ L_2 \\ | \\ F \end{array}\right\} \longrightarrow \operatorname{Aut}_{L_1} K \le \operatorname{Aut}_{L_2} K \le G$$

Thus a smaller fields yield largers groups, and vice-versa.

Theorem 15.3 (Fundamental Theorem of Galois Theory)**.** *Given K/F, a finite Galois extension with Galois group G then there is an inclusion reversing bijection ι such that*

$$\left\{\begin{array}{c} K \\ | \\ L \\ | \\ F \end{array}\right\} \qquad \begin{array}{ccc} L & \longrightarrow & \operatorname{Aut}_L K \\ & \iota & \\ K^H & \longleftarrow & H \end{array} \qquad \left\{\begin{array}{c} I \\ | \\ H \\ | \\ G \end{array}\right\}$$

and if $\iota(L) = H$ then $[L : F] = [G : H]$. This means that the lattice of subfields is the inverse of the lattice of subgroups (flip it upside-down).

15.2 Proofs

Theorem 15.4. *Let K be a field and let $H \leq \operatorname{Aut} K$ be a finite subgroup. Then K/K^H is finite and $[K : K^H] = \#H$.*

Proof. We already know that $H \leq \operatorname{Aut}_{K^H} K$. Now we only need to show that $[K : K^H] \leq \#H$. Suppose that $\#H = n$. Then given $\alpha_1, \dots, \alpha^m \in K$ with $m > n$ then $\alpha_1, \dots, \alpha^m$ are linearly dependent over K^H. WLOG, let $m = n + 1$. Write

$$H = \{\mathrm{id} = \sigma_1, \dots, \sigma_n\},$$

and consider the system of linear equations

$$\begin{aligned} \sigma_1(\alpha_1)x_1 + \cdots + \sigma_1(\alpha_{n+1})x_{n+1} &= 0 \\ &\vdots \\ \sigma_n(\alpha_1)x_1 + \cdots + \sigma_n(\alpha_{n+1})x_{n+1} &= 0 \end{aligned}$$

This is a system of n equations in $n + 1$ unknowns, and so it has a solution. We take some $\vec{v} \in K^{n+1}$ with minimal number of non-zero entries (minimal Hamming weight) and do some tricks. We permute the entries of $\vec{v}$ by σ_1 and show that this infact has a smaller Hamming weight and is still a solution, which is a contradiciton. ■

Corollary 15.5. *If K/F is a finite Galois extension with Galois group G and H is a subgroup of G then $[K : K^H] = \#H$. By the tower law, this says that $[K^H : F] = [G : H]$.*

16 Tuesday, 26 March 2019

Today's lecture was just random questions. Also, Grace Hopper is Awesome.

17 Thursday, 28 March 2019

17.1 Grace Hopper's Thesis