Math 612 Lecture Notes

Taught by Paul Gunnells, Notes by Patrick Lei

University of Massachusetts, Amherst

Spring 2019

Abstract

A continuation of Math 611. Topics covered will include field theory and Galois theory and commutative algebra. Prequisite: Math 611 or equivalent.

Contents

1 Organizational

A webpage (`http://people.math.umass.edu/~gunnells/alg/alg.html`) exists. There will be homework, one midterm, and a final. This course will cover fields, Galois theory, commutative algebra, and hopefully some homological algebra.

Warning: All jokes and conversations are reproduced as best as I can remember and my transcription is not necessarily faithful. In addition, footnotes and some definitions are based on my understanding of algebra and related topics.

2 Fields

2.1 Lecture 1 (Jan 22)

2.1.1 Basics

Definition 1 (Field)**.** A field is a commutative ring where every nonzero element is a unit.

Example 2. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all fields. However, $\mathbb{H}$ is not a field because it is non-commutative[1]. In addition, $\mathbb{Q}(\sqrt{2})$ is a field.

Example 3. For a prime p, $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ is a finite field.

Example 4. The field of fractions of any integral domain is a field. An example is $F(x)$ the field of fractions of $F[x]$ the polynomial ring over a field F. The field of fractions of $F[[x]]$ is $F((x))$, the formal Laurent series over F.

Definition 5 (Characteristic)**.** The characteristic of a field is the (positive) generator of the kernel of the unique ring homomorphism[2] $\mathbb{Z} \to F$. Alternately, it is the minimal positive integer such that $n \cdot 1 = 0$ in F.

Remark 6. Every field contains a prime field (either $\mathbb{Q}$ or $\mathbb{F}_p$).

Remark 7. Fields with positive characteristic are not finite in general. For example, consider $\mathbb{F}_p(x)$.

Definition 8 (Field Extension)**.** K is an extension of F is F is a subfield. We write K/F for this. Alternately, an extension is just a morphism of fields because every morphism of fields is injective.

Example 9. $\mathbb{F}_p(x)/\mathbb{F}_p$, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, $\mathbb{C}/\mathbb{R}$, and $\mathbb{R}/\mathbb{Q}$ are all field extensions.

Definition 10 (Degree of extension)**.** If K/F is a field extension, observe that K is an F-vector space. The degree $[K : F]$ of the extension K/F is the dimension of K over F.

Basically, all of algebraic number theory is about stuff like this: number fields and whatnot.

Theorem 11. *Let F be a field and $p \in F[x]$ irreducible. Then there exists K/F in which p has a root.*

Proof. Take $K = F[x]/(p(x))$. This is an extension of F and the class of x is a root of p. □

Remark 12. In the above theorem, observe that $[K : F] = \deg(p)$.

Example 13. Let $F = \mathbb{Q}$ and $p = x^3 + x^2 - 2x - 1$. We see that p is irreducible by the rational root theorem. Then $K = F[x]/(p)$ is a degree 3 extension of F and $p(\overline{x}) = 0$.

Paul proceeded to calculate the image of x^4 in K and say "It only took me ten times to get this right."

Example 14. Now let $F = \mathbb{F}_2$ and $p = x^2 + x + 1$. This is clearly irreducible because neither 0 nor 1 is a root, so $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2 + x + 1)$ is the field with 4 elements.

Paul calculated (half of) the addition and multiplication tables, stumbled over his words, and then proceeded to cite commutativity.

Remark 15. $\mathbb{F}_4 \not\cong \mathbb{Z}/4\mathbb{Z}$ but $\mathbb{F}_4 \simeq (\mathbb{Z}/2\mathbb{Z})^2$ as vector spaces over $\mathbb{F}_2$. Also, $\mathbb{F}_4^* \simeq \mathbb{Z}/3\mathbb{Z}$.

Remark 16. Any finite field is of the form $\mathbb{F}_q$ where q is a prime power. Also, there is a unique field of order q for any prime power q. In addition, F_q^* is cyclic.

[1] It is a division ring, or skew field

[2] $\mathbb{Z}$ is the initial object in the category of rings.

Paul remarked that we don't have the time to prove the above. However, this is easy to prove. He also said that he felt finite fields were glossed over in his education.

Definition 17 (Subfield generated by elements)**.** Let K/F be a field extension. Let $\alpha, \beta, \ldots \in K$. Then the field $F(\alpha, \beta, \ldots)$ is the smallest subfield of K containing F and $\alpha, \beta, \ldots$.

Definition 18 (Primitive element)**.** If $K \supset E = F(\alpha)$ for some $\alpha \in K$, then E is a simple extension and α is a primitive element.

Example 19. Let $K = \mathbb{R}, F = \mathbb{Q}$, and $E = \mathbb{Q}(\sqrt{2})$. Observe that the primitive element is not uniquely determined.[3]

We had a conversation:

Paul "Am I supposed to stop now?"

Suki "12:45."

Paul "I guess that was when the leaves were on the trees."

Example 20. Consider $\mathbb{Q}(\sqrt[3]{2})$. This is isomorphic to $\mathbb{Q}[x]/(x^3 - 2)$.[4]

Theorem 21. *Suppose K/F is an extension and $p \in F[x]$ irreducible has a root α in K. Then $F(\alpha) \simeq F[x]/(p)$.*

Proof. We have a morphism $F[x] \to F(\alpha)$ that sends $x \mapsto \alpha$. Observe that the kernel contains (p), so we get a map $F[x]/(p) \to F(\alpha)$. This is nonzero, so it must be injective. However, α is in the image, so the map must be surjective. □

During the proof of the last theorem, Paul made a comment about linear transformations and how we all thought it was disgusting even though it was the best part of last semester.

In the last 15 minutes, we will point out interesting things about fields. We've shown that $F[x]/(p)$ contains a root of p. In fact, the following remark holds:

Remark 22. Given any root α of p, then $F[x]/(p) \simeq F(\alpha)$. However, this field does not contain all the roots of p in general. If F is finite, then this field will contain all the roots.

"Let's stick with number fields because they're easier... we have more to play with with that."

Example 23. Let $F = \mathbb{Q}$. Then $\mathbb{Q}(\sqrt{2}) \simeq \mathbb{Q}[x]/(x^2 - 2)$ contains both roots of $x^2 - 2$. However, $\mathbb{Q}(\sqrt[3]{2}) \simeq \mathbb{Q}[x]/(x^3 - 2)$ contains only one root of $x^3 - 2$.[5]

Paul spent a long time discussing the second example and its one real and two complex embeddings.[6]

Example 24. $\mathbb{Q}[x]/(x^3 + x^2 - 2x - 1)$ contains all roots of $x^3 + x^2 - 2x - 1$. The roots are $x, x^2 - 2, -x^2 - x + 1$.

[3] However, by Dirichlet's primitive element theorem, every number field has a primitive element.

[4] This has one real and two complex embeddings.

[5] This is because of the statement in the previous footnote. The splitting field of $x^3 - 2$ is $\mathbb{Q}(\sqrt[3]{2}, \omega)$ where ω is a cube root of unity.

[6] Observe Dirichlet's unit theorem for the ring of integers of $\mathbb{Q}(\sqrt[3]{2})$.

The difference between the two examples are explained by Galois theory. Also, no homework has been assigned now and office hours have not been set.

2.2 Lecture 2 (Jan 24) Recall the idea of a field extension. Now we define an algebraic extension.

Definition 25 (Algebraic Extension)**.** Let K/F be an extension. Then let $\alpha \in K$. K/F is an algebraic extension if every element of K is algebraic over F.

If $\alpha \in K$ is not algebraic, it's called transcendental.

Definition 26 (Minimal Polynomial)**.** Let $\alpha \in K$ be algebraic over F. Then the minimal polynomial $m_{\alpha,F}(x)$ is the lowest-degree monic polynomial over F that has α as a root.

Proposition 27. *The minimal polynomial is uniquely determined.*

Proof. Suppose g is a minimal degree monic polynomial such that $g(\alpha) = 0$. Clearly g must be irreducible. Now suppose f is any other polynomial with $f(\alpha) = 0$. Then because $F[x]$ is Euclidean, we see that $f = qg + r$. Then we see that $r(\alpha) = 0$, but by minimality of the degree of g, $r = 0$. Therefore, $g \mid f$. □

Remark 28. The minimal polynomial $m_{\alpha,F}(x)$ depends on both α, F.

Example 29. The square root of 2 is algebraic over $\mathbb{Q}$, while the square root of -1 is algebraic over both $\mathbb{R}, \mathbb{Q}$ with minimal polynomial $x^2 + 1$.

Remark 30. Consider $\mathbb{R}/\mathbb{Q}$ as an extension. Then we see that $\mathbb{R} \cap \overline{\mathbb{Q}}$ is countable, so the set of transcendental real numbers is nonempty (in fact, algebraic numbers have measure zero). For example, π is transcendental by Lindemann. Another example is $x \in F(x)$.

Paul gave several more examples, but this one is the important one:

Remark 31. Finite degree extensions are algebraic.[7]

Proposition 32. *Let K/L and L/F be extensions. Then $[K : F] = [K : L][L : F]$.*

Proof. Let $\alpha_1, \ldots, \alpha_n$ be a basis for L/F and $\beta_1, \ldots, \beta_m$ be a basis for K/L. Then we will show that $\alpha_1\beta_1, \ldots, \alpha_n\beta_m$ is a basis for K/F. To see that the products span K, write $\lambda \in K$ as a linear combination of the β_i and then write each coefficient as a linear combination of the α_j.

Now we check that the products are linearly independent. Suppose we have $\sum c_{ij}\alpha_j\beta_i = 0$. Then we can pull back and get $\sum b_i\beta_i = 0$. But then each $b_i = 0$, so $\sum c_{ij}\alpha_j = 0$, which means that each $c_{ij} = 0$. □

Remark 33. The above proposition is also true if some extensions are infinite-degree.

Definition 34 (Finitely Generated)**.** Let K/F be an extension. Then K is finitely generated if there exits $\alpha_1, \ldots, \alpha_n \in K$ such that $K = F(\alpha, \ldots, \alpha_n)$.[8]

Lemma 35. $F(\alpha, \beta) = (F(\alpha))(\beta)$.

[7] To prove this, just use linear algebra on $1, \alpha, \alpha^2, \ldots$.

[8] In the number field case, this is all moot.

The proof of the above lemma is very long and Paul considers it a waste of time.

Theorem 36. *K/F is finite-degree if and only if it is finitely generated by algebraic elements.*

Proof. Assume K/F is finite. Then take an F-basis $\alpha_1, \dots, \alpha_n$. Then we see that $F \subset F(\alpha_i) \subset K$, so $[F(\alpha_i) : F] \mid [K : F]$. Thus α_i is algebraic. Then $K = F(\alpha_1, \dots, \alpha_n)$.

Now assume $K = F(\alpha_1, \dots, \alpha_n)$. Then we have a chain $F \subset F(\alpha_1) \subset \cdots \subset K$. Each inclusion is a finite extension, so K/F must be finite by multiplicativity. □

Definition 37 (Compositum)**.** Let $K_1, K_2 \subset K$ be subfields. Then the compositum K_1K_2 is the smallest subfield of K containing both K_1, K_2.

Proposition 38. *Suppose we have $F \subset K_1, K_2 \subset K$. Then if K_1, K_2 are finite over F, K_1K_2/F is also finite and $[K_1K_2 : F] \le [K_1 : F][K_2 : F]$.*

Proof. Suppose $K_1 = F(\alpha_1, \dots, \alpha_n), K_2 = F(\beta_1, \dots, \beta_n)$, where both expressions are for bases over F. Then $K_1K_2 = F(\alpha_1\beta_1, \dots, \alpha_n\beta_m)$. □

Remark 39. Equality holds when the products are linearly independent over F or $\gcd(m, n) = 1$.

2.2.1 Straightedge and Compass Paul believes that people still learn this in high school[9] and remarks that this is what numbers meant to the Greeks.[10] He then talked about how to construct numbers and mentioned that high schools lack straightedges and compasses[11] and send kids to GeoGebra. He then talked about computer help and joked that there must be a theorem that we need to prove.

There are a few things we can do with straightedge and compass:

1. Draw line between two points;
2. Make parallel lines;
3. Make perpendiculars;
4. If you can make a, b, you can make $a + b, ab, \frac{a}{b}, \sqrt{a}$.

Paul then constructed the lengths $ab, \frac{a}{b}, \sqrt{a}$ from a, b.

We can make any number a as long as a can be made using field operations and square roots.

"The Greeks had plenty of time. No internet, no TV, no Snapchat or whatever, nice weather, plenty of food."

Theorem 40. *If α is constructible, then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^k$.*

Remark 41. The converse of the above theorem is not necessarily true.

2.3 Lecture 3 (Jan 29)

[9] Sounds like he got an actual education

[10] Good thing we moved away from that and $\mathbb{R}$ is just the unique complete Archimedean field.

[11] My high school did have them.

2.3.1 Straightedge and Compass Continued Last time, we considered straightedge and compass constructions, where we can make all numbers in $\mathbb{R}$ that can be obtained from $\mathbb{Q}$ using field operations and square roots. For example, to construct a regular n-gon, we must construct $\cos(2\pi/n)$. In addition, we discussed degrees of field extensions formed from constructible numbers.

Some other classical problems[12] in ancient Greece were:

1. Doubling the cube: construct the cube root of 2. This is impossible because x^3-2 is irreducible.
2. Trisecting any angle: construct $\cos\frac{\theta}{3}$. Recall that $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$. This gives a cubic polynomial. If $\theta = \pi/9$, then this is impossible because our cubic is irreducible.
3. Squaring the circle: given a circle, make a square of the same area, i.e. construct the square root of π This is impossible because π is transcendental.

Paul says this is a nice application of the things we learned[13]

2.3.2 Spitting Fields

Definition 42 (Splitting Field)**.** Let $f \in F[x]$ and K/F be an extension. If f splits into linear factors over K but not over any proper subfield of K, then K is a splitting field of f.[14]

Example 43. $\mathbb{C}/\mathbb{R}$ is the splitting field of x^2+1, but $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not a splitting field for x^3-2.

"In the math department, we don't do any group hugging like other departments do."

Theorem 44. *Given any $f \in F[x]$, there exists a splitting field for it.*[15]

Proof. WLOG assume f is monic and irreducible. Then we know that $K = F[x]/(f(x))$ has at least one root of f, α. Then in $K[x]$, we have $f(x) = (x-\alpha)g(x)$ and continue by induction to obtain a field extension E/F where f splits. Now take the smallest subfield of E over which f splits. □

Corollary 45. *If E/F is a splitting field of f and $\deg f = n$, then $[E:F] \leq n!$.*

Proof. By construction and multiplicativity of degrees. □

Example 46. Let $\theta = \sqrt[3]{2}$, $F = \mathbb{Q}$, $f = x^3-2$, and $K = F(\theta)$.[16] To construct the splitting field E, we must adjoin ω. Thus $E \supset F(\omega) = L$. In fact, $E = LK$.

[12] These are all impossible, but proof of that took a long time to emerge.
[13] Imagine telling pure math students about applications.
[14] This is the initial object in the category of fields that split f.
[15] We will see that the splitting field is unique.
[16] This is one of Paul's top five favorite examples.

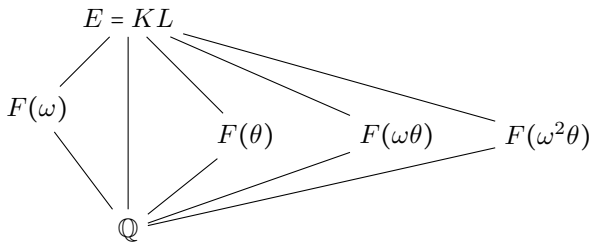


Figure 1: Subfields of $E = KL$

The connection between these subfields is explained by Galois theory. We will be spending a lot of time on Galois theory.

Theorem 47. *Splitting fields are unique up to isomorphism. If $f \in F[x]$, and E, E' are two splitting fields, then there exists an isomorphism $E \to E'$ that fixes F.*

We need a more general theorem:

Theorem 48. *Let $\varphi : F \to F'$ be an isomorphism of fields. Let $f \in F[x]$ and $f' \in F'[x]$ be its image under φ. Let E/F be a splitting field for f and E'/F' be a splitting field for f'. Then φ extends to an isomorphism $\sigma : E \to E'$.*

Proof. Let $n = \deg f$. If f splits already in $F[x]$, then f' does over F', so this case is trivial. Now assume the result for all f with degree less than n.

Let $p(x)$ be an irreducible factor of $f(x)$ of degree at least 2 and p' be the corresponding factor of f'. Let $\alpha \in E$ be a root of p and $\beta \in E'$ a root of p'. Then there exists an isomorphism $\sigma' : F(\alpha) \to F'(\beta)$ (remember that $F(\alpha) \simeq F[x]/(p(x)) \simeq F'[x]/(p'(x)) \simeq F'(\beta)$). Now we let $F_1 = F(\alpha)$ and $F_1' = F'(\beta)$, so we obtain the following commutative diagram:

$$\begin{array}{ccc} E & & E' \\ \uparrow & & \uparrow \\ F_1 & \xrightarrow{\sigma'} & F_1' \\ \uparrow & & \uparrow \\ F & \xrightarrow{\varphi} & F' \end{array}$$

By induction, we obtain an isomorphism $E \to E'$. □

"It's better to have an example without a theorem than a theorem without an example."

2.3.3 Algebraic Closure

Definition 49 (Algebraic Closure)**.** $\overline{F}/F$ is the algebraic closure of F if every $f \in F[x]$ splits completely in $\overline{F}[x]$ and in no smaller extension and $\overline{F}/F$ is an algebraic extension.

Definition 50 (Algebraically Closed)**.** If every $f \in K[x]$ has at least one root in K, then K is algebraically closed field.

Example 51. $\mathbb{C}$ is algebraically closed but is not the algebraic closure of $\mathbb{Q}$.

Our goal is to prove that every field has a unique algebraic closure. First we will show that every field is contained in an algebraically closed field and then we will take the smallesy subfield of K satisfying the definnition.

Proposition 52. *If $\overline{F}/F$ is an algebraic closure, then $\overline{F}$ is algebraically closed.*

Lemma 53. *If E/K and K/F are algebraic, then E/F is algebraic.*

"If you take nothing from this lecture besides the fact that I have terrible sweater-shirt combinations, it should be that the quotient of a ring by a maximal ideal is always a field."

Theorem 54. *Given any F, there exists an algebraically closed field containing F.*[17]

2.4 Lecture 4 (Jan 31)

2.4.1 Algebraic Closure Continued Recall the definitions of algebraically closed and algebraic closure from last time. We continue the proof of Theorem 54 from last time.

Proof of Theorem 54. Build K as a union of fields $F \subset K_1 \subset K_2 \subset \cdots$ with $K = \cup_i K_i$. Let $R = F[\ldots, x_f, \ldots]$, which is a polynomial ring with a variable x_f for each monic, nonconstant $f \in F[x]$. Let I be the ideal generated by $f(x_f)$ for all nonconstant monic f. We show this is a proper ideal. If not, then there exists an expression $\sum_i g_i f_i(x_{f_i}) = 1$. Passing to a finite extension F'/F such that each f_i has a root in F. Then this implies that $0 = 1$.

Now let $M \supset I$ be a maximal ideal and $K_1 = R/m$. Then every monic nonconstant polynomial has a root in K_1. K_1 may not be algebraically closed, so continue to form a tower of fields, and then let K be their union. We claim that K is algebraically closed. To see this, observe that every $f \in K[x]$ lives in $K_i[x]$ for some i. Then f has a root in K_{i+1}, so it has a root in K. □

Corollary 55. *Let F be a field and $K \supset F$ be algebraically closed. Let $\overline{F} \subset K$ be $\overline{F} = \{ \alpha \mid \alpha \text{ alg}/F \}$. Then $\overline{F}$ is the algebraic closure of F.*

Proof. Let $f \in F[x]$. Then $f = \prod(x - \alpha_i)$ where each $\alpha_i \in K$. In fact, each $\alpha_i \in \overline{F}$ because it is algebraic. □

Theorem 56. *Let F be a field. Then the algebraic closure $\overline{F}/F$ is unique up to isomorphism.*[18]

[17] This is proven in the next lecture.

[18] The proof of this is not given in the book and will not be given here.

2.4.2 (In)separability An intuitive way of thinking about this is that separable is nice and inseparable is not nice. Separable always happen in characteristic zero, but does not always happen in positive characteristics. Paul briefly mentioned the number field-function field analogy.

Let F be a field and E be the splitting field of $f \in F[x]$. In E we get a factorization $f = a_n \prod (x-\alpha_i)^{r_i}$. Then α is a simple root if it has multiplicity 1 and is a multiple root otherwise.

Definition 57. A polynomial $f \in F[x]$ is separable if it has no multiple roots in the splitting field E/F of f.

Example 58. Consider $f(x) = x^2 - 2 \in \mathbb{Q}[x]$. Then the splitting field is $\mathbb{Q}[\sqrt{2}]$ and f is separable.

Consider $x^2 + x + 1 \in \mathbb{F}_2[x]$. This splits in $\mathbb{F}_4$ as $x^2 + x + 1 = (x - \theta)(x - (1 + \theta))$, so it is separable.

Example 59. Consider the polynomial $x^2 - t \in \mathbb{F}_2(t)[x]$. Then this polynomial is inseparable (this is because $\sqrt{t} = -\sqrt{t}$).

How can we check for multiple roots? We take the formal derivative. "We aren't doing calculus here, but polynomials are really all we do in calculus class anyway." We define an operator $D_x : F[x] \to F[x]$ that sends a polynomial to its formal derivative. Then this operator satisfies the usual linearity and product rules.

Proposition 60. *α is a multiple root of f if and only if it is also a root of $D_x f$. In particular, the minimal polynomial of α divides both $f, D_x f$. Thus f is separable if and only if it is coprime with $D_x f$.*

Proof. Write $f = (x - \alpha)^n g(x)$ and differentiate. □

Example 61. $f(x) = x^n - 1$ is separable in characteristic 0 because it is coprime to $D_x f = nx^{n-1}$. In positive characteristic, if $p \nmid n$, f is separable. Otherwise if $p|n$, then the derivative is zero and every root is a multiple root.

Example 62. Consider $f = x^{p^n} - x \in \mathbb{F}_p[x]$. Then $D_x f = -1$, so there are no roots of $D_x f$ and f is separable.

Proposition 63. *Let* $\mathrm{char} F = 0$. *Then any irreducible f over F is separable.*

Proof. Suppose $\deg f = n$. Then the degree of $D_x f$ is -1. But then f is irreducible, so it must be coprime to $D_x f$. □

Remark 64. Proposition 63 is false in general in positive characteristic, but is true for finite fields. This allows us to distinguish finite fields and infinite fields of positive characteristic.[19]

Proposition 65. *Let F be of characteristic p. Then the Frobenius endomorphism is injective.*

Proof. It fixes 1, so it must be injective. □

Corollary 66. *The Frobenius endomorphism is an automorphism for any finite field F.*[20] *In fact, every element of F is a p-th power.*

[19] the thing that allows us to distinguish finite fields is important in number theory and geometry.
[20] This generates the Galois group of $F/\mathbb{F}_p$.

Definition 67 (Perfect Field)**.** K is a perfect field if either char $K = 0$ or if every element of K is a p-th power, where $p = \text{char } K$.

Proposition 68. *Every irreducible polynomial over a perfect field is separable.*[21]

2.5 Lecture 5 (Feb 5)

2.5.1 (In)separability Continued Recall the definition of a perfect field and a separable extension.

Proof of proposition 68. Assume that f is irreducible of degree n. Then consider $\gcd(f, D_x f)$. It can happen that $\deg D_x f < n - 1$. If we want $\gcd(f, D_x f) \neq 1$, then $D_x f = 0$. Therefore $f = g(x^p)$ for some $g \in K[x]$. Becuase K is perfect, every coefficient of g is a p-th power, which means that f must be a p-th power, so it is not irreducible. □

2.5.2 Classification of Finite Fields We will classify finite fields. Consider the splitting field E of $x^{p^n} - x$. This polynomial is separable, so E must contains exactly p^n roots. This forms a subfield of E (just check the field axioms). Therefore, E must be exactly the roots of $x^{p^n} - x$ and has order p^n, so $[E : \mathbb{F}_p] = n$. Therefore there exists a finite field of order any prime power.

Remark 69. $E \simeq \mathbb{F}_p[x]/(f)$ where f is irreducible. We can show by a counting argument that such f exist for all p, n.

However, note that $x^{p^n} - x$ splits completely over any finite field of order p^n (order of the group of units is $p^n - 1$). Therefore, finite fields are unique.

Remark 70.

1. We can perform the same construction starting with $\mathbb{F}_q$ for any prime power q.
2. We can also show that E^* is cyclic.
3. Any finite division ring is a field.

Proposition 71. *Suppose $f(x) \in F[x]$ is irreducible and that F has characteristic p. Then there exists a unique $k \geq 0$ and a unique irreducible polynomial $f_{sep}(x)$ such that $p(x) = p_{set}(x^{p^k})$.*

Proof. If f is separable, then $f_{sep} = f$ and $k = 0$. Otherwise, the derivative is zero and $f(x) = f_1(x^p)$. Then if f_1 is separable, $k = 1$ and $f_{sep} = f_1$. If not, we can continue. However, by well-ordering, this process must terminate with $f = f_k(x^{p^k})$. Now we show that f_k is irreducible. If not, then f cannot also be irreducible (just replace x with x^{p^k} in any factorization). □

Remark 72. f_{sep}, k are uniquely determined.

Definition 73 ((In)separable Degree)**.** The separable degree $\deg_s p(x) = \deg p_{sep}$ and the inseparable degree $\deg_i p(x) = p^k$.

We see that $\deg p = \deg_s p \cdot \deg_i p$. Observe that p is separable if and only if $\deg_s p = \deg p$.

Definition 74 (Purely Inseparable)**.** p is purely inseparable if $\deg_s p = 1$.

[21] We defer proof of this to next time. This is important for reasons of Galois theory.

Definition 75 (Separable Extension)**.** An algebraic extension is separable if all elements are roots of separable polynomials. Otherwise, the extension is inseparable.

Note that if F is perfect, then all algebraic extensions are separable. In general, given E/F algebraic, there exists a subfield $F \subset E_{sep} \subset E$ such that E_{sep}/F is the largest separable extension of F in E. If $E = F[x]/(f)$, then E_{sep} has degree $\deg_s f$. The extension E/E_{sep} is called purely inseparable.

Example 76. Consider the field $F = \mathbb{F}_2(t)$. Let $f = x^2 - t$ and $E = F[x]/(f)$. Note that $f(x) = f_{sep}(x^2)$, where $f_{sep} = x - t$. Thus E/F is purely inseparable.

Example 77. Again let $F = \mathbb{F}_2(t)$. Let $f = x^4 + tx^2 + t$. By Eisenstein, this polynomial is irreducible. Then note $f(x) = f_{sep}(x^2)$ where $f_{sep} = x^2 + tx + t$. Then $[E : E_{sep}] = [E_{sep} : F] = 2$.

2.5.3 Cyclotomic Fields Fix n. Then consider $\zeta_n = e^{2\pi i/n} \in \mathbb{C}$, which is algebraic ove $\mathbb{Q}$. Let $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ be the subfield of $\mathbb{C}$ containing $\mathbb{Q}$ and $e^{2\pi i/n}$ is the primitive n-th root of unity. We want to write $\mathbb{Q}(\zeta_n) = \mathbb{Q}[x]/(\Phi_n(x))$.

We will define a polynomial Φ_n and show that $\Phi_n | x^n - 1$, $\Phi_n \in \mathbb{Z}[x]$, Φ_n is irreducible, and $\deg \Phi_n = \varphi(n)$.

Define $\mu_n \subset \mathbb{C}$ be the group of all n-th roots of unity. Then clearly μ_n is cyclic generated by ζ. If $d|n$, then $\mu_d < \mu_n$ generated by $\zeta^{n/d}$. The other primitive n-th roots are $P = \{ \zeta^a \mid \gcd(a, n) = 1 \}$. Then $x^n - 1 = \prod_{\omega \in \mu_n} (x - \omega)$. Define $\Phi_n(x) = \prod_{\omega \in P} (x - \omega)$. Observe that $x^n - 1 = \prod_{d|n} \Phi_d(x)$. By construction, the first and fourth properties are true.

2.6 Lecture 6 (Feb 7)

2.6.1 Cyclotomic Fields Wrap-up Consider $\mathbb{Q}(\zeta_n)$ and recall the definition of the cyclotomic polynomial.

Theorem 78. *$\Phi_n(x) \in \mathbb{Z}[x]$ is irreducible with degree $\varphi(n)$.*

Proof. We proceed using induction. Suppose $\Phi_m \in \mathbb{Z}[x]$ for all $1 \le m < n$. Write $x^n - 1 = f(x)\Phi_n(x)$. Then $f(x) \in \mathbb{Z}[x]$ and divides $x^n - 1$ over $\mathbb{Q}$. Thus $\Phi_n \in \mathbb{Q}[x]$. Then by Gauss's lemma, $\Phi_n \in \mathbb{Z}[x]$.

To show that Φ_n is irreducible, assume not and write $\Phi_n = f(x)g(x)$ where f is irreducible. Let ζ be a primitive root that is a root of f and choose $p \nmid n$, so ζ^p is also a primitive root. Then suppose $g(\zeta^p) = 0$, so $g(x^p)$ is divisible by f. Then we work mod p and see that $(\overline{g}(x))^p \overline{g}(x^p) = \overline{f}(x)\overline{h}(x)$, so $\overline{f}$ and $\overline{g}$ have a common factor in $\mathbb{F}_p[x]$ and thus Φ_n has a multiple root mod p. However, this is not possible when $p \nmid n$. Therefore ζ^p is a root of f and similarly, ζ^a is a root for any a coprime to n. Thus $\Phi_n = f$. □

3 Galois Theory

3.1 Lecture 6 (cont.)

3.1.1 Basics The motivation behind Galois theory is to understand the structure of algebraic field extensions. Typical questions are:

1. What subfields $K \supset E \supset F$ can we have?
2. Can we understand invariants of them?
3. Suppose we have $K \supsetneq E \supsetneq F$. Can we construct it?

Our main tool for studying these questions is group theory.

Definition 79 (Galois Group)**.** Let K/F be an extension. Then $\mathrm{Aut}(K/F)$ is the group of automorphisms of K that fix F pointwise.

Example 80. $\mathrm{Aut}\,\mathbb{C}/\mathbb{R} \simeq \mathbb{Z}/2\mathbb{Z}$ and similarly for $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$.

Example 81. Let θ a root of $x^3 + x^2 - 3x - 1$. Then we see that the automorphism group is isomorphic to $\mathbb{Z}/3\mathbb{Z}$ generated by $\theta \mapsto \theta^2 - 2$.

Example 82. The automorphism group of $\mathbb{Q}[x]/(x^3 - 2)$ is trivial.

Example 83. The automorphism group of $\mathbb{F}_{p^n}/\mathbb{F}_p$ is isomorphic to $\mathbb{Z}/n/Z$ generated by the Frobenius endomorphism.

Example 84. Let $E/\mathbb{Q}$ be the splitting field of $x^3 - 2$. Then we can show that $\mathrm{Aut}\, E/\mathbb{Q} \simeq S_3$.

Question 85 (Inverse Galois Problem)**.** *Is every finite group the Galois group of an algebraic extension over the rationals?*

Proposition 86. *Let K/F be an extension with $\alpha \in K$ algebraic over F. Then if $\sigma \in \mathrm{Aut}\, K/F$, then $\sigma\alpha$ is a rot of the minimal polynomial of α.*

Proof. Let the minimal polynomial be $\sum a_i x^i$. Then $0 = \sigma\left(\sum a_i \alpha^i\right) = \sum \sigma(a_i \alpha^i) = \sum a_i (\sigma\alpha)^i$. □

Corollary 87. *If $f \in F[x]$ is irreducible with roots in K, then $\mathrm{Aut}\, K/F$ must permute them.*

Remark 88. σ may act trivially.

3.1.2 Correspondences Suppose $G = \mathrm{Aut}\, K/F$. Let $H \leq G$. Then H determines a subset $K_H \subset K$ defined by the set of elements fixed by H.

Proposition 89. *K_H is a subfield of K containing F.*

Proof. Left as an exercise to the reader.[22] □

We can also produce a subgroup corresponding to each subfield. These correspondences are inclusion-reversing.

Theorem 90. *1. If $H_1 \leq H_2$ then $K_{H_1} \supset K_{H_2}$.*

2. Of $E_1 \subset E_2$ then $\mathrm{Aut}\, K/E_1 \geq \mathrm{Aut}\, K/E_2$.

[22] Now I can write my own math textbook.

The proof of this theorem is straightforward. Ultimately, we will identify a class of "Galois extensions" for which these correspondences behave optimally.

Definition 91 (Galois Extension)**.** Let K/F be a finite extension. Then K is a Galois extension of F if $|\operatorname{Aut} K/F| = [K : F]$.

Example 92. Quadratic extensions of $\mathbb{Q}$ are Galois. So are the extensions $\mathbb{Q}[x]/(x^3 + x^2 - 2x - 1)$ of $\mathbb{Q}$ and $\mathbb{F}_{p^n}/\mathbb{F}_p$.

Example 93. The extension $\mathbb{Q}[x]/(x^3 - 2)$ is not Galois and neither is $E/\mathbb{F}_2(t)$ where $E = \mathbb{F}_2(t)[x]/(x^2 - t)$.

Example 94. Splitting fields of separable irreducible polynomials are Galois extensions. Thus the splitting field of any irreducible polynomial over a perfect field is Galois. Conversely, any Galois extension is the splitting field of a separable polynomial.

Proposition 95. *Let E/F be the splitting field of a polynomial $f \in F[x]$. Then $|\operatorname{Aut} E/F| \le [E : F]$ and equality holds if f is separable.*

3.2 Lecture 7 (Feb 12)

3.2.1 Correspondences Continued Last time, we discussed correspondences between subgroups of G and fields between K and F.

We will prove Proposition 95.

Proof of Proposition 95. Recall the proof of the uniqueness of splitting fields. We had this commutative diagram:

$$\begin{array}{ccc} E & \xrightarrow{\sigma} & E' \\ \uparrow & & \uparrow \\ F & \xrightarrow{\varphi} & F' \end{array}$$

We will show that the number of suitable σ is at most $[E : F]$. We use induction. Then the number of extensions is 1. Then let p be an irreducible factor of f of degree greater than 1. Then let p' be the corresponding factor of f'. Let α be a root of p. Then $F \subset F(\alpha) \subset E$. Then if σ is any isomorphism, we can restrict to an isomorphism $\tau : F(\alpha) \simeq F'(\beta)$. Then the following diagram commutes.

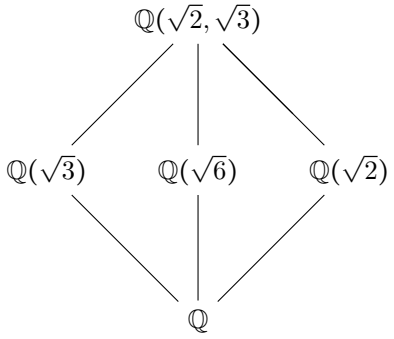
$$\begin{array}{ccc} E & \xrightarrow{\sigma} & E' \\ \uparrow & & \uparrow \\ F(\alpha) & \xrightarrow{\tau} & F'(\beta) \\ \uparrow & & \uparrow \\ F & \xrightarrow{\varphi} & F' \end{array}$$

Conversely, given any root β of p', we can make such a diagram. Then $\#\tau$ is at most $[F(\alpha):F]$. Use induction on the top half of the diagram and the result follows. $\square$

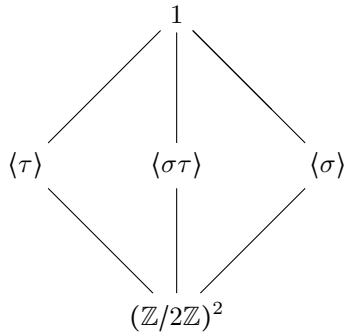
Eventually we see that K/F is Galois if and only if it is a splitting field of a separable polynomial.

Example 96. Consider $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$ for $D \in \mathbb{Z}$ squarefre. Then $\sqrt{D} \mapsto -\sqrt{D}$ is an automorphism and the Galois group of this extension is $\mathbb{Z}/2\mathbb{Z}$.

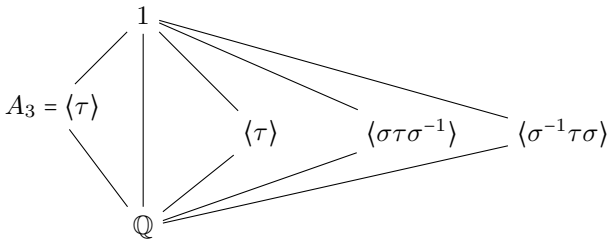
Example 97. Consider the field $\mathbb{Q}(\sqrt{2},\sqrt{3})$. Then the automorphisms $\sqrt{2} \mapsto -\sqrt{2}$ and $\sqrt{3} \mapsto -\sqrt{3}$ are nontrivial and have order 2. Thus the Galois group is $(\mathbb{Z}/2\mathbb{Z})^2$. Here is the subfield lattice.



Here is the subgroup lattice:



Example 98. Recall the splitting field of $x^3 - 2 = f$. Let θ be a root of f and ω be a root of Φ_3. Then $E = \mathbb{Q}(\omega,\theta)$. The total degree of this extension is 6 and thus $\mathrm{Aut}\,(E/F) = 6$. But then note that σ that sends $\theta \mapsto \omega\theta$ is of order 3, while τ that sends $\omega \mapsto \omega^2$. However, $\sigma\tau \neq \tau\sigma$, so the automorphism group is S_3. The subfield lattice is somewhere earlier in the notes, so I will just include the subgroup lattice:



Remark 99. Automorphisms in the previous example that act on $\mathbb{Q}(\omega)$ take it to itself while automorphisms that are nontrivial on the $\mathbb{Q}(\theta)$ do not preserve it. We will see that this is because A_3 is a normal subgroup of S_3 but $\mathbb{Z}/2\mathbb{Z}$ is not.

Our goal now is to prove the fundamental theorem of Galois theory. The idea is a complete characterization of the subgroup and subfield lattices. Today we will prove some of the technical results that we need.

Definition 100 (Character)**.** Let G be a group and L a field. Then a character χ of G with values in L is a homomorphism of groups $\chi : G \to L^\times$ (Note that this is completely governed by the abelianization of the group).

Definition 101 (Linear independence)**.** A collection $\chi_1, \dots, \chi_n$ is linearly independent if there does not exist a linear relation $\sum a_i\chi_i = 0$ where $a_i \in L$ and the a_i are not all 0.

Example 102. Let $G = \mathbb{C}^\times \times \mathbb{C}^\times$. Then we see that $\chi_1(a,b) = ab$ and $\chi_2(a,b) = a/b$ are linearly independent (if not, then b^2 is constant for all $b \in \mathbb{C}$).

Remark 103. Any character[23] of G is of the form $\chi(a,b) = a^n b^m$ for some fixed $n, m \in \mathbb{Z}$ and any finite subset if linearly independent.

Theorem 104. *Any finite subset of distinct characters $\chi_1, \dots, \chi_n$ is linearly independent.*

Proof. Take a minimal relation of the form $a_1\chi_1 + \cdots + a_m\chi_m = 0$ where all $a_i \neq 0$. Then for all $g \in G$, we have $a_1\chi_1(g) + \cdots + a_m\chi_m(g) = 0$. Then there exists $g_0 \in G$ such that $\chi_1(g_0) \neq \chi_m(g_0)$. Therefore, for all $g \in G$, $a_1\chi_1(g_0g) + \cdots + a_m\chi_m(g_0g) = 0$.

Thus, $a_1\chi_1(g_0)\chi_1(g) + \cdots + a_m\chi_m(g_0)\chi_m(g) = 0$. Then we must have $\sum_{i=2}^m a_i(\chi_i(g_0) - \chi_i(g_0))\chi_i(g) = 0$ for all $g \in G$. But this is a shorter length expression with not all coefficients zero, which contradicts minimality of the original relation. □

If we have a field homomorphism $\sigma : K \hookrightarrow L$, then this gives a character of $K^\times$.

Corollary 105. *Any distinct field embeddings are linearly independent.*

Corollary 106. *Distinct automorphisms of a field are linearly independent.*

3.3 Lecture 8 (Feb 14 ♡)

[23] Well, any algebraic character. For example, complex conjugation is an automorphism of $\mathbb{C}^\times$ that is not algebraic.

3.3.1 Towards the Fundamental Theorem of Galois Theory Our goal is to prove the Fundamental Theorem of Galois Theory. Recall the definition of a character and that any finite set of distinct characters is linearly independent. In particular, note that a collection of distinct field embeddings is linearly independent.

Now suppose $K = L$. Then any finite set of automorphisms is linearly independent.

Theorem 107. *Let $G = \{\sigma_i \mid 1 \le i \le n\}$ be a subgroup of $\operatorname{Aut} K$. Let $F \subset K$ be the fixed field. Then $[K : F] = |G| = n$.*

Proof. First suppose that $n > [K : F] = m$. Then let $\omega_1, \dots, \omega_m$ be an F-basis of K. Consider the linear system

$$\sum_{i=1}^{n} \sigma_i(\omega_j)\chi_i = 0,$$

where $j = 1, \dots, m$. Because there are fewer euqations than variables, there exists a non-trivial solution $(\beta_1, \dots, \beta_n) \in K^n$. Choose m arbitrary elements $a_1, \dots, a_m \in F$. Then $\sigma_i(a_k) = a_k$ for all i. In the linear system multiply the jth equation by a_j and substitute $\chi_i \leftarrow \beta_i$.

Now we have the linear system $\sum_{i=1}^{n} \sigma_i(a_j\omega_j)\beta_i = 0$. Adding the equations together, we obtain

$$\sum_{i=1}^{n} \sigma_i \left(\sum_{j=1}^{m} a_j\omega_j \right) \beta_i = 0.$$

Because the a_j are arbitrary, then we can put any element of K inside the σ_i. Therefore $\sum_{i=1}^{n} \sigma_i(k)\beta_i = 0$ for all $k \in K$, which is a nontrivial linear dependence on the σ_i, which is impossible.

Now we suppose that $n < [K : F]$. Then choose $\alpha_1, \dots, \alpha_{n+1}$ linearly independent over F and form a linear system

$$\sum_{i=1}^{n+1} \sigma_j(\alpha_i)\chi_i = 0,$$

where $j = 1, \dots, n$. There is a nontrivial solution, so let $(\beta_1, \dots, \beta_{n+1})$ be the solution. We claim that at least one β_i is in $K \setminus F$ (otherwise we have a linear dependence of the α_i using the β_i as coefficients). Now choose a solution with a minimum number of nonzero elements, say $r \le n + 1$. We can assume that $\beta_r = 1$.

We will form a new nontrivial solution with fewer nonzero elements. Assume without loss of generality that $\beta_1 \notin F$. Then the system becomes

$$\sigma_j(\alpha_r) + \sum_{i=1}^{r-1} \sigma_j(\alpha_i)\beta_i = 0.$$

We will choose $\sigma' \in G$ such that $\sigma'(\beta_1) \neq \beta_1$. Then note that left multiplication by σ' permutes the σ_i. Therefore, we apply σ' to our system and renumber. We now have the system

$$\sigma_j(\alpha_r) + \sum_{i=1}^{r-1} \sigma_j(\alpha_i)\sigma'(\beta_i) = 0.$$

Taking the difference of our two systems, we have the new equation

$$\sigma_j(\alpha_1)(\beta_1 - \sigma'(\beta_1)) + \cdots + \sigma_j(\alpha_{r-1})(\beta_{r-1} - \sigma'(\beta_{r-1})) = 0.$$

Because the first coefficient is nonzero, we now have a nontrivial solution with fewer nonzero elements. □

Corollary 108. *If K/F is finite, then $|\operatorname{Aut} K/F| \le [K:F]$. Then equality happens if and only if F is the fixed field of $\operatorname{Aut} K/F$.*

Proof. Let F' be the fixed field. Then by the theorem, $[K:F'] = |\operatorname{Aut} K/F|$. The desired result holds by multiplicativity. □

Corollary 109. *Let G be a finite group of automorphisms of K with fixed field F. Then $\operatorname{Aut} K/F = G$ and K/F is a Galois extension with Galois group G.*

Proof. Our assumptions imply that $G \le \operatorname{Aut} K/F$ and $|G| \le \operatorname{Aut} K/F$. Then recall that $|\operatorname{Aut} K/F| \le [K:F]$. Therefore $[K:F] = |G| \le |\operatorname{Aut} K/F| \le [K:F]$, so they are all equal. □

Corollary 110. *Let $G_1 \ne G_2$ be distinct subgroups of $\operatorname{Aut} K$. Let F_1, F_2 be the fixed fields. Then $F_1 \ne F_2$.*

Proof. Suppose $F_1 = F_2$. Then G_2 fixes F_1, so $G_2 \le G_1$. Similarly, $G_1 \le G_2$. Thus they are equal. □

The consequence of these is that taking fixed fields of different subgroups of $\operatorname{Aut} K$ gives different subfields of K over which K is Galois.

Theorem 111. *K/F is Galois if and only if K is the splitting field of a separable polynomial over F. Furthermore, if this is true then any polynomial over F with a root in K is separable and has all its roots in K.*

Proof. We already showed that Galois is implied by splitting field. Now assume K/F is Galois. Then $G = \operatorname{Gal}(K/F) \coloneqq \operatorname{Aut} K/F$. Write $G = \{1, \sigma_2, \dots, \sigma_n\}$. Let $p \in F[x]$ be irreducible with a root $\alpha \in K$. We show all the roots are in K. Consider the list $\{\alpha, \sigma_2\alpha, \dots, \sigma_n\alpha\}$. Assume the distinct elements in the orbit are $\alpha_1, \dots, \alpha_r$. It must be that $f(x) = \prod_{i=1}^{r}(x - \alpha_i) \in F[x]$. Then p is irreducible with root α, so p is the minimal polynomial of α over F. Then $p \mid f$ in $F[x]$. However, $f \mid p$ in $K[x]$. Therefore $p = f$ is separable and has all roots in K.

Now we prove that K/F is a splitting field. Assume K/F is Galois with group G. Then choose $\omega_1, \dots, \omega_n$ a basis of F over K. Let $p_1, \dots, p_n$ be the minimal polynomials over F of the ω_i. We know each is separable and has all its roots in K. Take g to be the LCM of the p_i. We see that g is squarefree, so it is separable. We see that K is the splitting field. The roots are all in K, so the splitting field is a subfield. The ω_i are all roots of g, so the splitting field is K. □

We have seen that the following are equivalent:

1. K is a Galois extension of F.
2. K is the splitting field of a separable polynomial in F;
3. K is an extension of F such that F is exactly the fixed field of $\operatorname{Aut} K/F$;

4. K is an extension of F such that $[K : F] = |\operatorname{Aut} K/F|$;
5. K is a finite, normal, and separable extension of F.

3.4 Lecture 9 (Feb 21) We will finally get to the Fundamental Theorem of Galois Theory.

Theorem 112. *Let K/F be a Galois extension with group G. Then there is an inclusion-reversing bijection between subfields of K containing F and subgroups of G. This correspondence takes a subfield to the subgroup fixing it and a subgroup to its fixed field. The bijection satisfies*

(a) $[G : H] = [E_H : F]$ and $|H| = [K : E_H]$;

(b) K/E is Galois with group $H_E \leq G$;

(c) E/F is Galois if and only if $H_E \trianglelefteq G$. In this case $\operatorname{Gal}(E/F) \simeq G/H_E$. Even if H_E isn't normal, the isomorphisms of E into an algebraic closure that fix F are in bijection with the cosets.

(d) If E_1, E_2 correspond to H_1, H_2, then $E_1 \cap E_2$ corresponds to (H_1, H_2) the subgroup generated by H_1H_2. The compositum E_1E_2 corresponds to the intersection $H_1 \cap H_2$. Therefore we have a correpondence between the subgroup lattice and the subfield lattice.

An example is the lattices for the splitting field of $x^3 - 2$ over $\mathbb{Q}$. These are somewhere earlier in the notes. Note that we have proven most of this theorem already.

Proof of Theorem 112. We have already shown most of this theorem. For example, we showed that the map from subgroups to subfields is injective. To see that is is surjective, choose a subfield E and suppose K/F is the splitting field of $f \in F[x]$. Then K/E is Galois and E is the fixed field of $\operatorname{Aut} K/E < G$.

Now we will show (c). Suppose E is the fixed field of $H \leq G$. Then for any $\sigma \in G$, take E to $\sigma(E)$, isomorphic to E fixing F. Let $\tau : E \to \tau(E)$ be an isomorphism in a fixed algebraic closure fixing F. Let $\alpha \in E$ have minimial polynomial $m_\alpha(x)$ over F. Then $\tau\alpha$ is another root of m_α. If K is the splitting field of $f \in F[x]$, then it is the splitting field of the same polynomial over E. Therefore it is the splitting field of τf over $\tau(E)$. But $\tau f = f$. Then by the uniqueness of splitting fields, we have a commutative diagram:

$$\begin{array}{ccc} K & \xrightarrow{\sigma} & K' \\ \uparrow & & \uparrow \\ E & \xrightarrow{\tau} & \tau(E) \\ \uparrow & & \uparrow \\ F & \xrightarrow{\mathrm{id}} & F \end{array}$$

Therefore, any such τ comes from $\sigma \in G$. When do σ, σ' give the same τ? Then $\sigma^{-1}\sigma' = \mathrm{id}$, which happens if and only if σ, σ' determine the same coset of H. Then the statement of normality follows. Part (d) is easy and is left to the treatment in D&F. □

3.4.1 Computing Galois Groups We use the following fact:

Proposition 113. *Let f be irreducible of degree n. Then define $\mathrm{Gal}(f) \coloneqq \mathrm{Gal}(E/Q)$, where E is the splitting field of f. Then $G = \mathrm{Gal}(f) \leq S_n$ and acts transitively.*

For example, if $n = 3$, then the only groups are S_3, A_3.

Example 114. Let $f = x^3 + 7x + 14$. Note that f has only one real root (derivative is always positive). Therefore, the two complex roots are conjugate, so there is an element of order 2 in the Galois group. Therefore, the Galois group of f is S_3.

Example 115. Let $F = \mathbb{Q}(\theta)$, where $\theta = \sqrt{2+\sqrt{2}}$. Note that $(\theta^2-2)^2 - 2 = 0$. Then our candidate polynomial is $f = x^4 - 4x^2 + 2$. This is irreducible by Eisenstein with roots $\pm\sqrt{2 \pm \sqrt{2}}$. We need to see whether $\sqrt{2-\sqrt{2}} \in F$. We see that $\sqrt{2} \in F$ and that $\sqrt{2+\sqrt{2}}\sqrt{2-\sqrt{2}} = \sqrt{2}$, so all roots are in $\mathbb{Q}(\theta)$. Therefore F is the splitting field of f. Then we see that either $G = \mathbb{Z}/4\mathbb{Z}$ or $G = (\mathbb{Z}/2\mathbb{Z})^2$. Then the automorphism σ that takes $\theta \to \alpha$ has order 4, so the group is $\mathbb{Z}/4\mathbb{Z}$.

Example 116. Consider $f = x^6 + 3$. This is irreducible by Eisenstein. Then take $\alpha = \sqrt{3}$ and $\rho = e^{2\pi i/12}$ a primitive twelfth root of unity.We see that the roots are $\rho\alpha, \ldots, \rho^{11}\alpha$. We determine if $\mathbb{Q}(r_1)$ is the splitting field. This is true if and only if the field contains ρ^2, which is true ($\sqrt{3} \cdot i = (\rho\alpha)^3$). Thus the extension has degree 6 and is either S_3 or $\mathbb{Z}/6\mathbb{Z}$.

3.5 Lecture 10 (Feb 26) There is an exam on March 7 in the evening. Topics will be announced later.

We finish the computation of the Galois group of S_3. Observe that complex conjugation is an automorphism of the extension. Then there exists another σ that sends $r_1 \mapsto r_2$. This has order 2, so the Galois group is S_3.

Note that if we set $f = x^6 + 2$, then this problem becomes must harder.

Example 117. Let $\theta = \sqrt{(2+\sqrt{2})(3+\sqrt{3})}$ and consider $K = \mathbb{Q}(\theta)$. Note that $\theta \notin \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Then we see that K is the splitting field, so the Galois group G has order 8. G must have at least three subgroups of order 4, so it can only be Q_8 or $(\mathbb{Z}/2\mathbb{Z})^2$. We can find an element of order 4, however $(\sqrt{(2+\sqrt{2})(3+\sqrt{3})} \mapsto \sqrt{(2-\sqrt{2})(3+\sqrt{3})})$, so $G = Q_8$.

Now if we try $\theta(a,b) = \sqrt{(a+\sqrt{a})(b+\sqrt{b})}$ with $a < b < 100$ prime, we get Galois groups:

Q_8 $(2,3), (2,19), (2,73)$;

$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$] $(2,5), (2,17), (2,37), (5.17), (5,37)$;

Order 16 $(2,7), (2,11), (2,13)$;

Order 32 $(3,11)$.

Note that the order 16 group is the almost direct product of $Q_8, \mathbb{Z}/4\mathbb{Z}$.

3.5.1 Finite Fields Recall that we can construct $\mathbb{F}_{p^n}/\mathbb{F}_p$ for all p, n, which is Galois. We will show that G is cyclic of order n.

Proposition 118. $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \simeq \mathbb{Z}/n\mathbb{Z}$ *and is generated by the Frobenius element.*

Proof. Consider orders of the Frobenius element. This is left as an exercise to the reader. □

Now we can consider a subextension $\mathbb{F}_{p^n}/\mathbb{F}_{p^d}$ where $d|n$. This has Galois group $\mathbb{Z}/(n/z)\mathbb{Z}$.

Proposition 119. $\mathbb{F}_{p^n}^\times$ *is cyclic.*

Proof. This is left as an exercise. Just consider the elements of order dividing $p^d - 1$ for $d|n$. □

Remark 120. The fact about roots you need to prove the previous proposition leads to the Miller-Rabin primality test.

Now recall that K/F is simple if it is generated by a primitive element.

Corollary 121. $\mathbb{F}_{p^n}/\mathbb{F}_p$ *is simple. This implies that there exists an irreducible polynomial of degree* n *over* $\mathbb{F}_p$.

Proof. Take a generator θ of the group of units. This generates the field extension. □

Remark 122. $x^{p^n} - x$ is the product of all irreducible polynomials of degree $d|n$. This will allow us to count the irreducible polynomials.

3.6 Lecture 11 (Feb 28) Last time we proved that all finite fields are simple extensions of $\mathbb{F}_p$.

Example 123. Let $p = 2$. Then $x^4 - x = x(x+1)(x^2+x+1)$ and $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.

To count irreducible polynomials over $\mathbb{F}^p$, we use Möbius inversion. Recall the Möbius function from number theory. Consider F, f on the positive integers. Then suppose $F = \sum_{d|n} f(d)$.

Theorem 124 (Möbius Inversion)**.** $f(n) = \sum_{d|n} \mu(d)F(n/d)$.

Let $\psi(n)$ be the number of irreducible polynomials of degree n over $\mathbb{F}_p$. Then note that $p^n = \sum_{d|n} d\psi(d)$. Therefore, $n\psi(n) = \sum_{d|n} \mu(d)p^{n/d}$, so $\psi(n) = \frac{1}{n}\sum_{d|n} \mu(d)p^{n/d}$. We can prove that $\psi(n) \neq 0$, but it's not clear that it is an integer.

Now we consider the algebraic closure $\overline{\mathbb{F}_p} = \bigcup_{n\geq 1} \mathbb{F}_{p^n}$, whic is infinite. Note that the subfields are ordered by divisibility.

3.6.1 Primitive Elements Our goal is now the primitive element theorem:

Theorem 125. *If* K/F *is finite and separable, then it is simple.*

Proposition 126. *Suppose* K/F *is Galois and let* F'/F *be any extension. Then* KF'/F' *is Galois with* $\mathrm{Gal}(KF'/F') \simeq \mathrm{Gal}(K/K \cap F')$.

Proof. We see that K is the splitting field of $f \in F[x]$. Then $f \in F'[x]$ and KF' is the splitting field of $f \in F'[x]$. Thus KF'/F' is Galois.

Consider the map $\varphi : G(KF'/F') \to G(K/F)$ given by restriction. Then σ fixes F', so it fixes F. Note that the kernel is all σ that restrict to the identity. Then σ is the identity on K and fixes F'

by construction, so is the identity on the composite. Therefore, φ is injective. Let K_H be the fixed field of the image. Then $K_H \supset K \cap F'$ However, it must be a subfield of F', so it must be equal to $K \cap F'$. □

Corollary 127. $[KF' : F] = \frac{[K:F][F':F]}{[K\cap F':F]}$.

Proof. We know that $[KF' : F'] = [K : K \cap F']$, so

$$\begin{aligned}[KF' : F] &= [KF' : F'][F' : F] \\ &= [K : K \cap F'][F' : F] \\ &= \frac{[K : F]}{[K \cap F' : F]}[F' : F].\end{aligned}$$

□

Proposition 128. *Let K_1, K_2 be Galois extensions of F. Then $K_1 \cap K_2/F$ and K_1K_2/F are Galois. The Galois group of K_1K_2/F is*

$$H = \{ (\sigma, \tau) \mid \sigma \in G(K_1/F), \tau \in G(K_2/F), \sigma|_{K_1\cap K_2} = \tau|_{K_1\cap K_2} \}.$$

Proof. Suppose $p \in F[x]$ is irreducible with a root in $K_1 \cap K_2$. Then all roots of p are in both K_1, K_2, so $K_1 \cap K_2/F$ is finite, normal, and separable. Now suppose K_i is the splitting field of separable polynomials f_i. Then K_1K_2 is the splitting field of the separable polynomial $\mathrm{LCM}(f_1, f_2)$, so it is Galois.

Now consider the map $G(K_1K_2/F) \to G(K_1/F) \times G(K_2/F)$ given by the product of the restrictions. First we see that this is injective. This is because anything in the kernel is trivial on both K_1, K_2, so it is the identity on the composite. Clearly, the image is in H because the restrictions of σ to K_1, K_2 agree on $K_1 \cap K_2$. To find the order, we see that $|H| = \frac{|G(K_1/F)||G(K_2/F)|}{|G(K_1\cap K_2/F)|}$. On the other hand, $[K_1K_2 : F] = [K_1K_2 : K_1][K_1 : K_1 \cap K_2][K_1 \cap K_2 : F] = [K_2 : K_1 \cap K_2][K_1 : F] = \frac{[K_2:F]}{[K_1\cap K_2:F]}[K_1 : F]$. □

A partial converse is that if $G(K/F) \simeq G_1 \times G_2$, then $K = K_1K_2$ where K_i is the fixed field of G_i.

Corollary 129. *Let E/F be finite and separable. Then there exists a Galois extension $K \supset E \supset F$ such that any Galois extension of F containing E is an extension of K.*

Proof. Take an F-basis $\alpha_1, \ldots, \alpha_k$ of E. Take their minimal polynomials and the composite of the splitting fields to take a Galois extension. Then take the intersection of all Galois extensions of F containing E to get the Galois closure. □

Example 130. $G(\mathbb{Q}(\sqrt{2}, \sqrt{3})) = (\mathbb{Z}/2\mathbb{Z})^2$.

3.7 Lecture 12 (Mar 5) The exam will be in LGRT 206 from 7-8 : 30 covering everything through section 14.2.

From last time, our goal is to prove the primitive element theorem.

Proposition 131. *Suppose K/F is finite. Then $K = F(\theta)$ if and only if there are only finitely many intermediate fields $K \supset E \supset F$.*

Proof. Let $K = F(\theta)$. Let f be the minimal polynomial and E be a subfield. Then let g be the minimal polynomial of θ in $E[x]$. Clearly $g|f$ in $E[x]$. Let E'/F be the field generated by the coefficients of g. Then $E' \subset E$ and the minimal polynomial of θ over E' is still g. Therefore $[K : E] = [K : E']$, so $E = E'$. Therefore subfields of K correspond to different monic fractions of f, of which there are only finitely many.

Now we assume there are only finitely many intermediate fields. We may also assume F is infinite. We show that a primitive element exists for $F(\alpha, \beta)$, which is sufficient by induction. Consider the fields $\{F(\alpha + c\beta) \mid c \in F\}$. Given that there are only finitely many intermediate fields, there exist $c, c' \in F$ such that $F(\alpha + c\beta) = F(\alpha + c'\beta)$. Then we see that $\alpha, \beta \in F(\alpha + c\beta)$, so $F(\alpha, \beta) = F(\alpha + c\beta)$. □

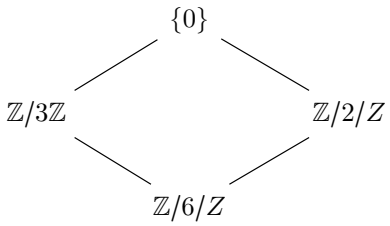
We will now prove the finite element theorem.

Proof of Theorem 125. Take the Galois closure K of E/F. Then $[K : F]$ is finite, which means there are only finitely many subfields between K and F. In particular, there must be only finitely many subfields between E and F. Now use the proposition. □

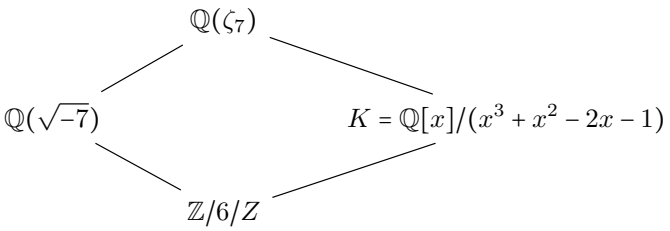
3.7.1 Cyclotomic Fields Let ζ_n be a primitive nth root of unity. Then recall the nth cyclotomic polynomial $\Phi_n(x) \in \mathbb{Q}[x]$, which is irreducible of degree $\phi(n)$.

We will show that $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois with $G \simeq (\mathbb{Z}/n\mathbb{Z})^\times$. Define a morphism $(\mathbb{Z}/n/Z)^\times \to \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ given by $a \mapsto \sigma_a$. Analyzing this, we see that this is an isomorphism. Paul claims that this is not canonical.

Example 132. Consider $\mathbb{Q}(\zeta_7)$. Then $G \simeq \mathbb{Z}/6\mathbb{Z}$. The subgroups have order $1, 2, 3, 6$. Therefore the subgroup lattice is:



The subfield lattice is:



Now suppose p is an odd prime and let $H \leq G = (\mathbb{Z}/p\mathbb{Z})^\times$. We can define $\alpha_H = \sum_{\sigma\in H}\sigma(\zeta_n)$. This is invariant under H and generates the fixed field of H. Note that this does not in general because the primitive nth roots need not be linearly independent over $\mathbb{Q}$.

Example 133. Let $p = 7$. Then note that $\mathbb{Z}/2\mathbb{Z}$ is generated by $\zeta \mapsto \zeta^6 = \overline{\zeta}$. Then the fixed field is clearly real. To find the generator, note that $(\zeta+\zeta^{-1})^3 = \zeta^3+3\zeta+3\zeta^{-1}+\zeta^{-3}, (\zeta+\zeta^{-1})^2 = \zeta^2+2+\zeta^{-2}$. Then recall that $\zeta+\zeta^2+\zeta^3+\zeta^{-1}+\zeta^{-2}+\zeta^{-3} = -1$. Using these facts, it is easy to see that $\zeta+\zeta^{-1}$ satisfies x^3+x^2-2x-1.

Also, we can see that $\alpha_{\mathbb{Z}/3\mathbb{Z}} = \zeta+\zeta^2+\zeta^4$. Then it is straightforward to find the minimal polynomial, which is quadratic of discriminant -7.

Now recall that ϕ is multiplicative. Then we will see that $\mathbb{Q}(\zeta_n)$ is the compositum of the $\mathbb{Q}(\zeta_{p_i^{e_i}})$.

Theorem 134 (Kronecker-Weber)**.** *If $F/\mathbb{Q}$ is Galois with abelian Galois group, there exists n such that $F \subset \mathbb{Q}(\zeta_n)$.*

Example 135. $\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\zeta_p)$ if $p \equiv 1 \pmod 4$.

Remark 136. This theorem is false if $\mathbb{Q}$ is replaced by any other ground field. Find an explicit example is an open problem, but we do have a classification of abelian extensions of a number field.

Remark 137.
1. We can show that any finite abelian group appears as a Galois group over $\mathbb{Q}$. The proof is to see G as a quotient of $(\mathbb{Z}/n\mathbb{Z})^\times$ for some n.
2. To construct an n-gon, we need to make ζ_n using our straightedge and compass. This is possible if and only if $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ has order 2^k. Then $\mathbb{Q}(\zeta_n)$ is the top of a tower of a series of quadratic extensions. Therefore $\phi(n)$ is a power of 2. This means that $\phi(n) = 2^k$, which means that $n = 2^m p_1\cdots p_t$ where $p_i = 2^r+1$ a Fermat prime. Only 5 Fermat primes are known: $3, 5, 17, 257, 65537$.

3.8 Lecture 13 (Mar 19)

Recall that the Galois group of a polynomial is the Galois group of its splitting field.

Proposition 138. *Suppose f is irreducible and separable of degree n. Then* $\mathrm{Gal}(f)$ *acts transitively on the roots.*

Proof. Let α, β be two roots. Then $F(\alpha) \simeq F(\beta)$, so if K/F is the splitting field, then this isomorphism extends to an automorphism of K. □

This implies that $\mathrm{Gal}(f) \hookrightarrow S_n$ and the image acts transitively on the roots.

Example 139. If $n = 3$, the possible Galois groups are S_3 and $A_3 = \mathbb{Z}/3\mathbb{Z}$.

If $n = 4$, the possible Galois groups are $S_4, A_4, D_8, V_4, Z/4\mathbb{Z}$.

Remark 140. $V_4 \trianglelefteq A_4 \trianglelefteq S_4$ and $V_4 \trianglelefteq S_4$. For $n \neq 4$ the only normal subgroup of S_n is A_n and A_n is simple for $n \neq 4$.

Note that if f is reducible, then $\mathrm{Gal}(f)$ is not n-transitive, but injects into a product of symmetric groups corresponding to each irreducible factor.

The general principle is that the generic irreducible over $\mathbb{Q}$ of degree n has Galois group S_n. We can't prove this because we can't make this notion precise for now.

Let $x_1, \ldots, x_n$ be variables. Then $(x - x_1)(\cdots(x - x_n))$ is the generic polynomial of degree n. This is a polynomial in $F(x_1, \ldots, x_n)[x]$. Denote $F_x = F(x_1, \ldots, x_n)$. Recall the elementary symmetric functions. Then $f = \prod(x - x_i) = x^n - s_1x^{n-1} + x_2x^{n-2} + \cdots + (-1)^n s_n$. Now consider $F(s_1, \ldots, s_n) = F_s$. Now we have a field extension F_x/F_s. Also, F_x is the splitting field of f and S_n acts on the x_i and fixes the s_i. Thus the fixed field of S_n contains F_s, so the extension is Galois with Galois group S_n.

Corollary 141. *If $f(x_1, \ldots, x_n)$ is symmetric, then f is a rational function in the s_i.*

Proof. $f \in F_s$, so it must be rational in the s_i. □

Remark 142. If $f \in \mathbb{Z}[x_1, \ldots, x_n]$ is symmetric, then $f \in \mathbb{Z}[s_1, \ldots, s_n]$. Note that this is not true for the power basis.

Now let $s_1, \ldots, s_n$ be indeterminates and consider $f \in F_s[x]$. Suppose $x_1, \ldots, x_n$ are roots of f.

Proposition 143. *There are no polynomial relations over F among the x_i.*

Proof. Suppose $p(x_1, \ldots, x_n) = 0$. Let $\widetilde{(p)} = \prod_{\sigma \in S_n} p(t_{\sigma(1)}, \ldots, t_{\sigma(n)}) \in F[t_1, \ldots, t_n]$. Then $\widetilde{(p)}$ is symmetric and $\widetilde{p}(x_1, \ldots, x_n) = 0$. Therefore we obtain a relation on the s_i with F-coefficients, which is impossible. □

This shows that if the coefficients of a polynomial are indeterminates, then so are its roots. The converse is also true (proved later in the text).

Theorem 144. *The polynomial $x_n - s_1x^{n-1} + \cdots \pm s_n$ is separable with Galois group S_n.*

Note this is not enough to say that generically the Galois group is S_n because that statement depends on the base field F. For $F = \mathbb{Q}$, this works. However, if F is finite, this does not work.[24]

Now consider $A_n \trianglelefteq S_n$. Then there is a quadratic extension of F_s corresponding to $\mathbb{Z}/2\mathbb{Z}$. Now consider the discriminant $D = \prod_{i<j}(x_i - x_j)^2 \in F_s$ and $\sqrt{D} = \prod_{i<j}(x_i - x_j)$, which is not S_n-invariant but is A_n-invariant.[25] Thus $E = F_s(\sqrt{D})$ (Here we assume $\mathrm{char}F \neq 2$).

Now we can define the discriminant of a polynomial $f \in \mathbb{Q}[x]$ with roots $\alpha_1, \ldots, \alpha_n$. Then $D \in \mathbb{Q}$ and if $\sqrt{D} \in \mathbb{Q}$, then $\mathrm{Gal}(f) \subset A_n$.

[24] He called 13 a giant number.

[25] D&F define the sign of a permutation this way.

3.9 Lecture 14 (Mar 21) Last time we discussed the discriminant of a field. We look at $n \leq 4$. If $n = 2$, then $f = x^2 + ax + b = (x - \alpha)(x - \beta)$. Then the discriminant is $D = a^2 - 4b$. If D is a rational square, f is reducible. Thus the Galois group is S_2 if and only if f is irreducible, and $A_2 = 1$ if and only if f is reducible.

Let $n = 3$. If f is reducible, it factors into either three linear factors or a linear and quadratic factor. The Galois group is either trivial or $\mathbb{Z}/2\mathbb{Z}$. Now suppose f is irreducible. Then $G \leq S_3$ is 3-transotive, and the Galois group is determined by the discriminant.

Consdier $f = x^3 + ax^2 + bx + c$. Take the transformation $x \to y - a/3$, which kills the quadratic term. This gives a polynomial $g(y) = x^3 + px + q$. This translation preserves differences of roots, so it preserves the discriminant. We calculate the roots. Note that $D = -g'(\alpha)g'(\beta)g'(\gamma)$, and we can compute that this is eaual to $27\alpha^2\beta^2\gamma^2 + 9p(\alpha^2\beta^2\gamma^2) + 3p^2(\alpha^2 + \beta^2 + \gamma^2) + p^3 = -4p^3 - 27q^2$.

If D is a square, then the Galois group is A_3, otherwise, S_3.

Example 145. Let $f = x^3 + x^2 - 2x - 1$. The discriminant is 49. On the other hand, the discriminant of $x^3 - x^2 + 1$ is -23.

Now consider $n = 4$. If f is reducible, we have the following cases:

- 4 linear factors: $G = 1$
- quadratic factor, 2 linear factors: $G = \mathbb{Z}/2\mathbb{Z}$
- cubic factor and linear factor: $G = S_3$ or $G = A_3$
- 2 quadratic factors: $G = \mathbb{Z}/2\mathbb{Z}$ or $G = (\mathbb{Z}/2\mathbb{Z})^2$

If f is irreducible, the possible groups are:

- S_4;
- A_4 (normal);
- $D_8 = \{1, (1324), (1423), (13)(24), (14)(23), (34), (12), (12)(34)\}$;
- $V_4 = \{1, (12)(34), (13)(24), (14)(23)\}$ (normal);
- $C_4 = \{1, (1234), (13)(24), (1432)\}$;

We need to be much more clever to compute the discriminant. We can always kill the cubic term by the transformation $x = y - a/4$. Thus we can take $g(y) = y^4 + py^2 + qy + r$. To compute the discriminant, we use the resolvent cubic. Let $\alpha_1, \ldots, \alpha_4$ be the roots of g. Set

$$\theta_1 = (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4)$$
$$\theta_2 = (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4)$$
$$\theta_3 = (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3)$$

Each θ_i is stabilized by exactly one of the three conjugate D_8. Thus V_4 stabilizes all θ_i. Also, all elementary symmetric functions of the θ_i are fixed by S_4. These are $2p, p^2 - 4r, -q^2$. Define the resolvent cubic to be $h(x) = x^3 - 2px^2 + (p^2 - 4r) + q^2$. We can show that h, g have the same discriminant.

Now we analyze h.

1. If h is irreducible, then $G(h) = S_3$ or A_3.
   (a) If S_3, then $G \not\leq A_4$ and 6 divides the size of G. Thus $G = S_4$.
   (b) If A_3, then $G \leq A_4$ and 3 divides the order of G. Thus $G = A_4$.
2. h is reducible.
   (a) h has 3 linear factors. Then $\theta_i \in \mathbb{Q}$, so $G \leq V_4$ and thus $G = V_4$.
   (b) h has a linear factor and a quadratic factor. Then θ_1 (WLOG) is rational. Thus G fixes θ_1 byt not θ_2, θ_3, so $G \leq D_8$ and $G \neq V_4$. Then either $G = D_8$ or C_4. Consider $D_8 \cap A_4 = V_4$, but $C \cap A_4 = \mathbb{Z}/2\mathbb{Z}$. The different intersections reflect the behavior of g considered as a polynomial over $\mathbb{Q}(\sqrt{D})$. If g is irreducible, $G = D_8$. If g is reducible, then $G = C_4$.

Example 146. Let $f = x^4 - 4x^2 + 9$. The resolvent cubic is $x^3 + 8x^2 - 20x = x(x+10)(x-2)$.

Example 147. For more examples (with examples), go to `www.lmfdb.org/NumberField/?degree=4`

3.10 Lecture 15 (Mar 26) There is only about a week and a half left of Galois theory.[26] The section concludes with the fundamental theorem of algebra. There is no proof of this fact that does not use topology or analysis. Gunnells says a better proof is the one using Liouville's theorem.

3.10.1 Solvable and Radical extensions Recall that G is solvable if there exists a chain of subgroups $1 \lhd G_1 \lhd \cdots \lhd G_r = G$ such that G_{i+1}/G_i is cyclic. IF G is solvable, then quotients and subgroups of G are solvable. Also, if $H, G/H$ are solvable, then so is G.

Example 148. S_3 is solvable: $1 \lhd \mathbb{Z}/3\mathbb{Z} \lhd S_3$. Also, S_4 is solvable: $1 \lhd \mathbb{Z}/2\mathbb{Z} \lhd S_4V_4 \lhd A_4 \lhd S_4$. Also, any finite abelian group is solvable.

Example 149. S_n is not solvable for $n \geq 5$ because A_n is simple.

The term "solvable" comes from Galois theory. We will see that a polynomial is solvable in radicals if and only if its Galois group is solvable.

Example 150. In degrees $2, 3, 4$ there are formulas for the roots of f in terms of the coefficients.[27]

Definition 151 (Simple Radical Extension)**.** K/F is a simple radical extension if $K = F(\sqrt[n]{a})$ for some $a \in F$.

Observe that a simple radical extension is Galois if and only if it is a splitting field of $x^n - a$. Therefore F must contain the n-th roots of unity.

[26] Commutative algebra is going to suck.

[27] Paul says that the quadratic formula is one of the first ways to see if someone is a math person. If one asks for formulas for higher degree polynomials, they're in trouble. Also, back in the day, people used to send each other challenge problems, and there was one guy who found the formula and sent cubics to other people as challenge problems. This also led to the development of complex numbers because they could not be avoided when finding roots of cubics. WARNING: This is complete revisionist history, but Paul claims he can do this because this is not a history class.

Proposition 152. *Let F have characteristic prime to n and suppose $\mu_n \subset F$. Then K/F is cyclic and $[K:F]$ divides n.*

Proof. We know the group is Galois. Then fix a root $\sqrt[n]{a} \in K$ and let $\sigma \in G(K/F)$. Therefore $\sigma(\sqrt[n]{a}) = \zeta_\sigma \sqrt[n]{a}$. This gives a map $G(K/F) \to \mu_n$. This is clearly a homomorphism, which proves the result. □

Proposition 153. *Any cyclic extension of degree n over a field F with $\mathrm{char} F \nmid n$ with $\mu_n \subset F$ is of the form $F(\sqrt[n]{a})$ for some $a \in F$.*

Proof. Let K be such and extension and $G(K/F) = \langle \sigma \rangle$. For any $\alpha \in K$ and $\zeta \in \mu_n$, we define the Lagrange resolvent

$$(\alpha, \zeta) = \sum_{k=0}^{n-1} \zeta^k \sigma^k(\alpha).$$

We note that $\sigma(\alpha, \zeta) = \zeta^{-1}(\alpha, \sigma)$. Also, $\sigma(\alpha, \zeta)^n = (\alpha, \zeta)^n$. Therefore $(\alpha, \zeta)^n \in F$. We know that $1, \sigma, \ldots, \sigma^{n-1}$ are linearly independent, so $(\alpha, \sigma) \neq 0$. Also $\sigma^i(\alpha, \zeta) = \zeta^{-i}(\alpha, \zeta)$. Therefore if ζ is primitive, $(\alpha, \zeta) \in K$ but not any subfield. Therefore $K = F((\alpha, \zeta))$. □

We now assume the characteristic of F is 0.

Definition 154 (Solvability in Radicals)**.** Let α be algebraic over F. We say α can be solved in radicals if there exists a tower $F = K_0 \subset K_1 \subset \cdots \subset K_r = K$ where $K_{i+1} = K_i(\sqrt[n_i]{a_i})$.

Definition 155. A polynomial can be solved in radicals if all of its roots can be.

Theorem 156. *$f \in F[x]$ can be solved in radicals if and only if $\mathrm{Gal}(f)$ is solvable.*

Lemma 157. *If $\alpha \in K$ is in a root extension, then α is contained in a root extension Galois over F.*

Proof. Let L be the Galois closure of K over F. If $\sigma \in \mathrm{Gal}(L/F)$, we get $F = \sigma K_0 \subset \cdots \subset \sigma K_r = \sigma K$ is still a root extension. We will take the compositum of the Galois conjugates of K. We need to show that the compositum of two root extensions is a root extension. This follows by induction on each chain of extensions. We conclude that $F = K_0 \subset \cdots \subset K_r = K$ and we can assume that K/F is Galois.

We need successive extensions to be cyclic. Let $F' \supset F$ containing μ_N for N large enough. Now we take the compositum KF'. We get $F \subset F' = F'K_0 \subset F'K_1 \subset \cdots \subset F'K$. Also $F'K/F$ is Galois because it is the composite of two Galois extensions. We can see that $F'K/F$ is a root extension. At each step, the Galois groups are cyclic. □

Proof of Theorem 156. Assume f is solvable in radicals. Then make the root extensions, take the Galois closure, and apply the lemma. Then use the fact that quotients of solvable groups are solvable to get that the splitting field of f is solvable. □

3.11 Lecture 16 (Mar 28) We finish the proof of Theorem 156 from last time.

Galois group is solvable implies polynomial is solvable. Suppose the Galois group is solvable. Then we take the splitting field of f and take the fixed fields $F = K_0 \subset K_1 \subset \cdots \subset K_r = K$. We know that K_{i+1}/K_i is cyclic and set $[K_{i+1} : K_i] = n_i$. Then choose F'/F a large enough cyclotomic extension, so we take $F \subset F' = F'K_0 \subset \cdots \subseteq F'K_r = F'K$. Therefore $F'K_{i+1}/F'K_i$ is cyclic of degree dividing n_i. Thus the roots of f can be solved in radicals. □

Remark 158. There shows that there do not exist formulas in radicals for an extension with Galois group A_5. However, if we allow things like modular forms, formulas exist. See Felix Klein's *Lectures on the Icosahedron.*

We are now almost done with Galois theory, which brings Paul great sadness.

3.11.1 Galois groups over $\mathbb{Q}$ We will leverage[28] the relationship between $\mathbb{Z}$ and $\mathbb{F}_p$. Let $f \in \mathbb{Z}[x]$ be separable of degree n. Then let $G = \mathrm{Gal}(f)$. We know $G \hookrightarrow S_n$. Then each $\sigma \in G$ determines a cycle type (conjugacy class), which is a partition $n = n_1 + \cdots + n_k$

Now take the discriminant D of f. If $p|D$, then $D \equiv 0 \mod p$, so f is not separable mod p. Then $p \nmid D$ implies that $D \not\equiv 0 \mod p$, so f is separable.

Proposition 159. *Suppose $f = f_1 \cdots f_k$ when reducing mod p. If f_i has degree n_i, then G contains an element of cycle type $n_1, \ldots, n_k$.*

This follows from

Theorem 160. *Let p not divide the discriminant of f. Then* f $\mod$ p $\hookrightarrow \mathrm{Gal}(f)$.

We vary p and consider the collection of cycle types.

Example 161. Consider $x^3 - x + 1$.

p	cycle type
2	3
3	3
5	2 1

Figure 2: Factorization in finite fields of $x^3 - x + 1$

We see the Galois group is S_3.

Example 162. Consider $x^5 - x + 1$.

[28] Business people love this word.

p	cycle type
2	3 2
3	5
5	5
7	3 2
11	5
163	2 1 1 1

Figure 3: Factorization in finite fields of $x^5 - x + 1$

We see the Galois group is S_5.

Now there are many possible cycle types that can apear in the list. Do all possible cycle types appear in the list?

Theorem 163. *All possible cycle types appear. The Chebotarev density theorem implies the following: Let T be a cycle type in G. Let $d_T = n_T/N$, where $N = |G|$ and n_T is the number of elements of G with cycle type T. Then*

$$\lim_{p\to\infty} \frac{\#\{p \mid f \mod p \text{ has cycle type } T\}}{\#\{p\{} = d_T.$$

In other words, the natural density of the cycle type equals the probability that a group element has that cycle type.

We take primes less than 10^6, of which there are 78498.

Example 164. Consider $x^3 - x + 1$.

cycle type	frequency	probability
1 1 1	13032	0.16602
1 2	39310	0.50078
3	26155	0.3332

Figure 4: Frequency of Cycle Types for $x^3 - x + 1$

Example 165. Consider $x^3 + x^2 - 2x - 1$.

cycle type	frequency
1 1 1	26153
1 2	0
3	52344

Figure 5: Frequency of Cycle Types for $x^3 + x^2 - 2x - 1$

Example 166. For $x^5 - x + 1$, the cycle type 1112 appears 6505 times, or 0.08287. For S_5, with f irreducible, the only possible groups are $\mathbb{Z}/5\mathbb{Z}, D_{10}, A_5, S_5, F_{20}$.

4 Commutative Algebra

The goal is to develop enough commutative algebra to study algebraic geometry and algebraic number theory. For a better treatment of the algebraic geometry/commutative algebra, see my notes for Jenia's class.

4.1 Lecture 17 (Apr 02)

Definition 167 (Noetherian Ring)**.** R is a Noetherian ring if it satisfies the ascending chain condition.

Recall that every nonzero chain of ideals contains a maximal ideal. This normally requires Zorn, but becomes automatic for Noetherian rings.

Example 168. If R is Noetherian, then $R[x]$ is Noetherian. In particular, If K is a field, then $K[x_1, \dots, x_n]$ is Noetherian.

Theorem 169. *The following are equivalent:*

1. *R is Noetherian.*
2. *Every nonempty set of ideals ordered by inclusion contains a maximal element.*
3. *Every ideal is finitely generated.*

Definition 170 (k-algebra)**.** R is a k-algebra if it is a ring and there is an injection K to the center of R.

Example 171. Consider the polynomial algebra $R = k[x_1, \dots, x_n]$. This an infinite dimensional vector space but a finite dimensional algebra.

Proposition 172. *R is a finitely generated K-algebra if and only if there exists a surjective map of K-algebras $K[x_1, \dots, x_n] \to R$ for some n.*

Proof. Let $r_1, \dots, r_n$ be generators. Then consider the map $K[x_1, \dots, x_n] \to R$ given by $x_i \mapsto r_i$. On the other side, if there is a surjective map, the images of the x_i generate R. □

Now let K be a field and $\mathbb{A}^n$ be the affine n-space over K. Then $f \in k[x_1, \dots, x_n]$ can be viewed as a k-valued function on $\mathbb{A}^n$.

Definition 173. $K[x_1, \dots, x_n]$ is the coordinate ring $k[\mathbb{A}^n]$ of $\mathbb{A}^n$ where each x_i serves as a coordinate function on $\mathbb{A}^n$.

Definition 174. $V \subset \mathbb{A}^n$ is an affine algebraic set if there exists $S \subset K[\mathbb{A}^n]$ such that $V = \{a \in \mathbb{A}^n \mid f(a) = a \text{ for all } f \in S\}$. We write $V = \mathcal{Z}(S)$.

Example 175. If S consists of a quadratic polynomial in 3 variables, the $\mathcal{Z}(S)$ is a quadric surface.

Note that $\mathcal{Z}$ depends on the field, even though S might make sense over many fields.

Example 176. Consider $\mathbb{A}^2$ and $S = \{y\}$. Then over $\mathbb{R}$ we get a line, over $\mathbb{C}$ we get the plane, and over $\mathbb{F}_p$ we get a set of points.

Example 177. If $S = \{f\} \subset k[\mathbb{A}^2]$ then $\mathcal{Z}(S)$ is a plane curve. In general if S contains 1 element, we call $\mathcal{Z}(S)$ a hypersurface.

We can check the following results:

1. If $S \subset T$ then $\mathcal{Z}(S) \supset \mathcal{Z}(T)$;
2. If S generates the ideal S, then $\mathcal{Z}(S) = \mathcal{Z}(I)$.
3. $\mathcal{Z}(S) \cap \mathcal{Z}(T) = \mathcal{Z}(S \cup T)$.
4. Let I, J be ideals. Then $\mathcal{Z}(I) \cup \mathcal{Z}(J) = \mathcal{Z}(IJ)$.
5. $\mathcal{Z}(0) = \mathbb{A}^n$ and $\mathcal{Z}(1) = \varnothing$.

We now have a map $\mathcal{Z} : \{\text{ideals}\} \to \{\text{affine varieties}\}$. However, this is not injective.

Example 178. $\mathcal{Z}((x)) = \mathcal{Z}((x^2)) = \{0\} \subset \mathbb{A}^1$.

Proposition 179. *$V \subset \mathbb{A}^n$ is the intersection of finitely many hypersurfaces.*

Proof. $V = \mathcal{Z}(I)$ for some ideal I, which is finitely generated by Noetherianness of $k[x_1, \dots, x_n]$. Then I is the intersection of the hypersurfaces given by the generators. □

We have a map $\mathcal{I}$ in the other direction from $\mathcal{Z}$ sending an affine variety to the ideal of all functions that vanish on it. This map is not surjective. We determine the image of $\mathcal{I}$. We will answer the question in the case when K is algebraically closed.

Definition 180. Let V be an affine variety. Then the quotient $K[\mathbb{A}^n]/\mathcal{I}(V)$ is called the coordinate ring $K[V]$ of V.

Morally, we want $K[V]$ to be the set of polynomial functions on V. These come from restricting polynomials from $\mathbb{A}^n$ to V (and the kernel must be $I(V)$). We see that subsets and quotients are dual notions.[29]

The next question we want to answer is when two affine varieties are isomorphic. First we need to define what a morphism is.

Definition 181. A morphism, or regular map, between two affine varieties V, W is a function $\varphi : V \to W$ given by polynomial functions. In other words, there exist polynomials $\varphi_1, \dots, \varphi_m \in K[\mathbb{A}^n]$ such that $\varphi = (\varphi_1, \dots, \varphi_m)$.

Now that we have the notion of a morphism, we can define an isomorphism in the usual way. Next time we will prove that two affine varieties are isomorphic if and only if their coordinate rings are isomorphic.

[29] "This is something nobody tells you until I just did."

4.2 Lecture 18 (Apr 04) Last time we discussed some basic algebraic geometry.[30] Given two affine varieties V, W, a map $\varphi : V \to W$ induces a pullback $\widetilde{\varphi} : K[W] \to K[V]$. Verifying that this construction is well-defined is omitted from these notes.[31] In fact, the pullback is a map of K-algebras. The converse to this construction is that for any K-algebra homomorphism $K[W] \to K[V]$, we have a corresponding morphism of varieties $V \to W$.[32]

Theorem 182. *There is a bijection between regular maps $V \to W$ and K-algebra morphisms $K[W] \to K[V]$ given by the pullback. This is a contravariant functor that gives an equivalence of categories between affine varieties and finitely generated K-algebras with no nilpotent elements.*[33]

Example 183. Consider $V = \mathbb{A}^1$, $W = \mathcal{Z}(x^3 - y^2) \subset \mathbb{A}^2$ and let $\varphi : V \to W$ be given by (t^2, t^3). Then the pullback sends $K[W]$ to $K[t^2, t^3]$, so the map is a bijection but not an isomorphism.[34]

Paul proceeded to talk about the difference between the origins in V, W topologically. For reference, see Milnor's *Singular points on complex hypersurfaces.*

4.2.1 Radical ideals We know we have the $\mathcal{Z}$ correspondence between ideals and affine varieties and the $\mathcal{I}$ correspondence in the other direction. There are not bijections. In particular, $\mathcal{I}(\mathcal{Z}(I)) \neq I$ in general. There is a relation between the two ideals though.

Definition 184. The radical of I is the ideal $\{a \in R \mid a^k \in I \text{ for some } k \geq 1\}$. The radical of 0 is called the nilradical, and I is called radical if $I = \sqrt{I}$.

Example 185. The radical of (x^2) is (x).

Example 186. The nilradical is the set of nilpotent elements of R.

Proposition 187. *1. $\sqrt{I}$ is an ideal contining I.*

2. $\sqrt{I}$ descends to the nilradical of R/I.

3. R/I has no nonzero nilpotents if and only if I is radical.

4.3 Lecture 19 (Apr 09) Last time we stated Proposition 187. The proof is obvious (just use the binomial theorem for the first part, and the the other parts follow).

Proposition 188. *$\sqrt{I} = \cap P$ where P runs over all prime ideals containing I.*

Proof. We pass to the quotient and prove the analogous theorem for the nilradical. If a is in the nilradical, then $a^k = 0 \in P$, so a is in any prime ideal. Now if a is not in the nilradical, then consider all ideals not containing any positive power of a, which includes the zero ideal. Then S contains a maximal element by Zorn (upper bound is union). Then this maximal element is prime. □

Corollary 189. *All prime ideals are radical.*

[30] As in chapter 3 of Reid.

[31] Differential geometry class is just this for two terms. You just pull things back over and over again.

[32] For reference, see Reid's book.

[33] This last part is from a conversation with Jenia.

[34] This is birational, and the local ring at the origin is modified. Also, how many times have I seen this example? (Luca, Reid, Jenia, Shafarevich, Paul)

Proposition 190. *Suppose R is Noetherian and let $I \subset R$ be an ideal. then for some $k \geq 1$, we have $(\mathrm{rad} I)^k \subset I$. In particular, the nilradical is a nilpotent ideal.*

Proof. Choose generators for the the radical. Then each generator x_i has $x_i^{n_i} \in I$, so if k is large enough, all k-ary products of the generators will be in I. □

Recall $k[V]$ for an affine variety. We see that the nilradical of $K[V]$ is trivial because every element of $k[V]$ is a function on V. Therefore the $\mathcal{I}$ correspondence has target radical ideals. However, $\mathcal{I}$ is still not surjective in some cases (for example $\mathbb{R}$). If $k = \mathbb{C}$, then this works.

Theorem 191 (Nullstellensatz)**.** *If k is algebraically closed, then* $\mathrm{im}\mathcal{I}$ *is exactly the radical ideals. Equivalently, $\mathcal{I}(\mathcal{Z}(I)) = \sqrt{I}$. We have a bijection between affine varieties and radical ideals.*

4.3.1 Zariski Topology We take for granted the notion of a topology.

Definition 192. The Zariski topology on $\mathbb{A}^n$ is given by defining the closed sets to be affine varieties.

Remark 193. The Zariski topology is course and not Hausdorff.

Remark 194. The Zariski topology on an arbitrary affine variety is the subspace topology from the Zariski topology on $\mathbb{A}^n$.

4.4 Lecture 20 (Apr 11) Recall the Zariski topology from last time. The Zariski topology on any affine variety is the subspace topology inherited from $\mathbb{A}^n$. We also know that regular maps are continuus in the Zariski topology. The Zariski closure and density are defined as usual for topology.

Proposition 195. *Let $A \subset \mathbb{A}^n$. Then $\overline{A} = \mathcal{Z}(\mathcal{I}(A))$.*

The proof of this is clear.

Proposition 196. *Let $\varphi : V \to W$ be regular and $\widetilde{\varphi}$ be the pullback. Then*

1. $\mathrm{Ker}\widetilde{\varphi} = \mathcal{I}(\varphi(V))$*;*
2. *The Zariski closure of $\varphi(V)$ is $\mathcal{Z}(\mathrm{Ker}(\varphi))$.*

For proof of this, see my notes for Jenia's class.

Define an reducible/irreducible affine algebraic set in the usual way. Then define an algebraic variety to be an irreducible affine variety.[35]

Proposition 197. *V is an algebraic variety precisely when $\mathcal{I}(V)$ is prime.*

Corollary 198. *V is a variety if and only if $K[V]$ is an integral domain.*

Definition 199. The function field $K(V)$ is the field of fractions of $K[V]$.

Note that this is a coarser invariant than the coordinate ring. Also, functions in $K(V)$ are not defined on all of V.

[35] This is not standard. Normally we assume our varieties to be projective or quasi-projective.

Recall that for a field extension E/F a subset $\{a_1, \dots, a_n\}$ are algebraically independent over F if $f(a_1, \dots, a_n) \neq 0$ for all $f \in F[x_1, \dots, x_n]$. A transcendence base for E/F is a maximal algebraically independent subset, and the transcendence degree is the cardinality of the transcendence base.

Definition 200. The dimension of V is the transcendence degree of $K(V)$ over K.

Example 201. The dimension of $\mathbb{A}^n$ is n.

4.4.1 Integral elements and Integral Closure

Definition 202. Let $R \subset S$.

1. $s \in S$ is integral if it is a root of some monic polynomial over R.
2. S/R is integral if every $s \in S$ is integral over R.
3. The integral closure of R in S is the subset of all elements integral over R.
4. R is integrally closed in S if it equals its integral closure in S. If R is an integral domain, it is integrally closed (or normal) if it is integrally closed in its field of fractions.

Example 203. $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$.

Example 204. $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K for any number field K.

4.5 Lecture 21 (Apr 16) We continue our discussion of integrality.

Proposition 205. *The following are equivalent:*

1. *$s \in S$ is integral over R.*
2. *$R[s]$ is a finitely-generated R-module.*
3. *$s \in T$ for a subring $R \subset T \subset S$ that is a finitely generated R-module.*

Proof. First we show (1) $\Rightarrow$ (2). Suppose we have a polynomial $p(x) = x^n + \sum_{k=1}^{n} a_k x^{n-k}$. We know that $R[x]$ is generated by $1, s, s^2, \dots$, and $s^n = -\sum a_k s^{n-k}$, so $R[s]$ must be finitely generated.

To show (2) $\Rightarrow$ (3), take $T = R[s]$. Finally, to show (3) $\Rightarrow$ (1), let $v_1, \dots, v_n$ be a generating set for T. Then $sv_i = T$, so $sv_i = \sum_{j=1}^{n} a_{ij} v_j$ for $i = 1, \dots, n$. Therefore we have a system of linear equations

$$\sum (\delta_{ij} s - a_{ij}) v_j = 0$$

for $i = 1, \dots, n$. We use Cramer's rule, and get that the matrix $B_{ij} = \delta_{ij} s - a_{ij})$ has determinant 0, which gives a monic polynomial with s as a root. □

Corollary 206. *1. If $s, t \in S$ and are integral over R, then $st, s \pm t$ are integral over R.*

2. *The integral closure of R in S is a subring.*
3. *Integrality is transitive.*

Proof. We know $R[s], R[t]$ are finitely generated, and thus so is $R[s,t]$. This gives the first two parts.

For the last part, take $t \in T$. Then we can find $p(x) \in S[x]$ monic with $p(t) = 0$. Then each coefficient is integral over S, so we can take $R[a_1, \dots, a_n, t]$, which is finitely generated. Thus t is integral over R. □

Corollary 207. *The integral closure of R in S is integrally closed in S.*

Definition 208. Let $\varphi : R \to S$ be a morphism and I, J be ideals.

1. If $I \subset R$, then the extension of I to S is $\varphi(I)S \subset S$.
2. If $J \subset S$, then the contraction to R is the ideal $\varphi^{-1}(J) \subset R$.

If φ is injective, then we know $I \subset IS \cap R$ and $(J \cap R)S \subset J$, but these do not have to be equalities. Also, if $Q \subset S$ is prime, then its preimage is prime in R. This is not necessarily true if $P \subset R$ is maximal. Also, if $P \subset R$ is prime, $\varphi(P)S$ is not necessarily prime (for an example, consider splitting of rational primes in number fields).

Theorem 209. *Suppose $R \subset S$ is an integral extension.*

1. *Assume S is a domain. Then R is a field if and only if S is a field.*
2. *Suppose $P \subset R$ is prime. Then there exists a prime ideal $Q \subset S$ with $P = Q \cap R$. Then P is maximal if and only if Q is maximal.*
3. *(Going up theorem). Suppose we have an ascending chain of prime ideals $P_1 \subset P_2 \subset \cdots \subset P_n \subset R$. Then suppose we have a chain $Q_1 \subset \cdots \subset Q_m$, $m < n$ where Q_i are prime and $P_i = Q_i \cap R$ for $i \le m$. Then we can extend the chain to get $Q_1 \subset \cdots \subset Q_n$ with $Q_i \cap R = P_i$.*
4. *(Going down theorem). This is the same as going-up but with descending chains.*

Proof.

1. Suppose R is a field and $s \in S$ is nonzero. Then $s^{-1} \in S$. We can write $s^n + a_{n-1}s^{n-1} + \cdots + a_0 = 0$, where $a_i \in R$. We can assume $a_0 \neq 0$. Then we can find an inverse for s.

   Now suppose S is a field. Then we know $r \in R$, $r^{-1} \in S$ is integral, so we can wirte $r^{-m} + a_{m-1}r^{-m+1} + \cdots + a_1 r^{-1} + a_0 = 0$. Multiplying by r^{m-1}, we see that $r^{-1} \in R$.

2. This is proven in the text, so we omit the proof. We verify the maximal statement. Consider $R/p \subset S/Q$. Then we induce an integral extension on the quotients, and then use the first part to get the desired result.

3. We check that we can extend by 1, so consider $P_1 \subset P_2$. Consider $\overline{S} = S/Q_1, \overline{R} = R/P_1$. Then $\overline{S}/\overline{R}$ is integral and P_2/P_1 is prime in $\overline{R}$. By part 2, there exists, $\overline{Q_2} \subset \overline{S}$ prime with $\overline{Q_2} \cap \overline{R} = \overline{P_2}$. Lifting to R, S, $\overline{Q_2}$ is lifted to a prime $Q_2 \in S$ with $Q_2 \cap R = R_2$.

4. This is left as an exercise.

□

Definition 210. The ring of integers $\mathcal{O}_K$ of a number field K is the integral closure of $\mathbb{Z}$ in K.

Proposition 211. *$\alpha \in K$ is in $\mathcal{O}_K$ if and onlf if its minimal polynomial of α over $\mathbb{Q}$ has coefficients in $\mathbb{Z}$.*[36]

Proof. If the minimal polynomial is integral, then clearly $\alpha \in \mathcal{O}_K$. Assume α is integral in $\mathcal{O}_K$ and let $f \in \mathbb{Z}[x]$ be the minimum degree polynomial with α as a root that is monic. If f is not irreducible, then $f = gh$ and $g, h \in \mathbb{Z}[x]$ by Gauss. This contradicts the minimality of the degree of f, so f is irreducible and thus the minimal polynomial. □

Theorem 212. *Let K be a number field of degree n. Then*

1. *$\mathcal{O}_K$ is Noetherian.*
2. *$\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n.*
3. *Given $\beta \in K$, there exists $d \in \mathbb{Z}$ such that $d\beta \in \mathcal{O}_K$.*
4. *If $\beta_1, \dots, \beta_n$ is a $\mathbb{Q}$-basis of K, then there $d \in \mathbb{Z}$ such that $d\beta_i$ are a $\mathbb{Z}$-basis of a rank n free submodule of $\mathcal{O}_K$. Moreover, any $\mathbb{Z}$-basis of $\mathcal{O}_K$ is a $\mathbb{Q}$-basis of K.*

4.6 Lecture 22 (Apr 18)

We begin by proving Theorem 212.

Proof of Theorem 212. We prove the third part. Take $\beta \in K$ and let $x^m + \cdots + a_0 \in \mathbb{Q}[x]$ with β a root. Choose $d \in \mathbb{Z}$ large enough to cleaer all denominators, and then multiply both sides by d^m. Rewriting the polynomial in terms of dx, we see that $d\beta$ is integral over $\mathbb{Z}$.

Now to prove the fourth part, choose $\beta_1, \dots, \beta_n \in K$ and choose $d \in \mathbb{Z}$ large enough such that $d\beta_1, \dots, d\beta_n \in \mathcal{O}_K$. Because they are linearly independent over $\mathbb{Q}$, they must be linearly independent over $\mathbb{Z}$. Therefore they generate a rank n submodule of $\mathcal{O}_K$. To see that $\mathcal{O}_K$ is torsion-free we show it is contained in a finitely generated free $\mathbb{Z}$-module. Let L/K be the Galois closure, so we show that $\mathcal{O}_L$ is contained in a finitely generated $\mathbb{Z}$-module, so let $\alpha_1, \dots, \alpha_m$ be the $\mathbb{Q}$-basis of L. Clear denominators and we can assume $\alpha_i \in \mathcal{O}_L$.

Choose $\theta \in L^\times$ and define $T_\theta : L \to \mathbb{Q}$ by $\alpha \mapsto \mathrm{Tr}_{L/\mathbb{Q}}(\theta\alpha)$. Recall that the trace is a map onto $\mathbb{Q}$. This is not the zero map, so we have a morphism $L \to \mathrm{Hom}(L, \mathbb{Q})$. This is injective, so every linear form on L is a trace. Let $\alpha_1', \dots, \alpha_m'$ be the dual basis. Now choose $\beta \in \mathcal{O}_L$. We know that $\mathrm{Tr}(\alpha_j\beta) \in \mathbb{Z}$ because $\alpha_j, \beta \in \mathcal{O}_L$. Thus $\mathcal{O}_L \subset \mathbb{Z}\alpha_1' + \cdots + \mathbb{Z}\alpha_1'$ is contained in a finitely generated $\mathbb{Z}$-module, which is free. Therefore $\mathcal{O}_K$ is free with rank at most n. We showed $\mathcal{O}_K$ contains a module of rank n, so its rank is n.

We finally show $\mathcal{O}_K$ is Noetherian. Any ideal is a $\mathbb{Z}$-submodule of a free module of rank n, so it is free with finite rank and is thus finitely generated as an ideal. □

Definition 213. A $\mathbb{Z}$-basis of $\mathcal{O}_K$ is called an integral basis.[37]

Definition 214. K is monogenic if there exists $\theta \in \mathcal{O}_K$ such that $\mathcal{O}_K = \mathbb{Z}[\theta]$.

Example 215. Any quadratic number field and any cyclotomic field is monogenic.

[36] Here we assume the minimal polynomial is monic.

[37] Finding an integral basis for a given K is a fundamental problem in algebraic number theory.

Example 216. The field generated by the polynomial $x^3 + x^2 - 2x - 8$ is not monogenic, due to Dedekind.

4.6.1 Nullstellensatz Recall the $\mathcal{I}$ and $\mathcal{Z}$ constructions.

Theorem 217. *$\mathcal{Z}$ and $\mathcal{I}$ are inverse bijections between affine algebraic sets and radical ideals.*

Lemma 218 (Noether Normalization Lemma)**.** *Let K be a field and A a finitely generated K-algebra. Then there exist some algebraically independent elements $y_1, \dots, y_q \in A$ such that A is integral over $K[y_1, \dots, y_q]$.*[38]

Proof. If the generators r_i are algebraically independent, we are done. Otherwise, find a polynomial relation among the r_i: $f(r_1, \dots, r_m) = 0$ where $f \in K[x_1, \dots, x_m]$. Consider f as a polynomial in x_m with coefficients in $K[x_1, \dots, x_{m-1}]$. We assume f is nonconstant. We take new variables $X_i = x_i - x_m^{(1+d)^i}$, where d is the degree of f. Set $\alpha_i = (1+d)^i$.

Then we set $g(X_1, \dots, X_{m-1}, x_m) = f(X_1 + x_m^{\alpha_1}, \dots, X_{m-1} + x_m^{\alpha_{m-1}}, x_m)$. We observe that g has the form $cx_m^N + \sum_{i=0}^{N-1} h_i(X_1, \dots, X_{m-1}) x_m^i$, where $c \neq 0$.

Now set $s_i = r_i - r_m^{\alpha_i}$. Then we know r_m is integral over $B = K[s_1, \dots, s_{m-1}]$ and we know each r_i is integral over $B[r_m]$, so A is integral over $B[r_m]$. By induction on m, we get the desired result. □

4.7 Lecture 23 (Apr 23) We continue the proof of Noether normalization in last Thursday's notes.

Example 219. Let $r_1 = x^2, r_2 = xy, r_3 = y^2$. Then we have $r_1 r_3 = r_2^2$, so $f(x_1, x_2, x_3) = x_1 x_3 - x_2^2$. We see $d = 2$, so $\alpha_1 = 3, \alpha_2 = 9$. We can write $-g(X_1, X_2, x_3) = -f(X_1 + x_3^3, X_2 + x_3^9, x_3) = x_3^{18} + 2X_2 x_3^4 - X_1 x_3 + X_2^2$. Thus r_3 is integral over $K[x^2 - y^6, xy - y^{18}]$.

Now we prove the following:

Theorem 220 (Algebraic Nullstellensatz)**.** *An ideal $M \subset k[x_1, \dots, x_n]$ is maximal if and only if $M = (x_1 - a_1, \dots, x_n - a_n)$.*

Proof. If M is maximal, consider $E = A/M$, which is a field. Then E/K is generated by the images of the x_i. However, it must be a field, so there are no variable generators by Noether normalization. Then E is integral over K, so it is an algebraic extension. K is algebraically closed, so $E = K$. Therefore each x_i maps to a constant, so $x_i - a_i \in M$. Thus M contains $(x_1 - a_1, \dots, x_n - a_n)$, so it must equal M. □

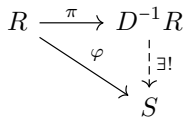
Theorem 221 (Nullstellensatz)**.** *$\mathcal{I}(\mathcal{Z}(I)) = \sqrt{I}$ if k is algebraically closed. Moreover, $\mathcal{I}, \mathcal{Z}$ give bijections between affine algebraic sets and radical ideals.*

Proof. For proof, see my notes to Jenia's class. Alternatively, see Reid. □

[38] While Paul was talking about this, my phone went off and he said "We welcome our new alien overlords".

4.7.1 Localization

Theorem 222. *Let R be a commutative ring with identity and D be a multiplicative subset. Then there exists a commutative ring $D^{-1}R$ and a map $\pi : R \to D^{-1}R$ such that if $\varphi : R \to S$ is a map of rings and $\varphi(D) \subset S^\times$, then there exists a unique map that makes the following diagram commute:*



Proof. Define localization in the usual manner. Define $D^{-1}R = \{(r,d) \mid r \in R, d \in D\}/\sim$, where $(r,d) \sim (s,e)$ if $x(re - sd) = 0$ for some $x \in D$. □

Corollary 223.
1. $\ker \pi = \{r \in R \mid xr = 0 \text{ for some } x \in D\}$, *so π is injective if and only if $0 \notin D$ and no zero divisors are in D.*
2. *$D^{-1}R = 0$ if and only if $0 \in D$ if and only if D contains nilpotent elements.*

Example 224. The first example is the field of fractions of an integral domain. Also, we can localize at some nonzero $f \in R$; we write $D^{-1}R = R_f$. Note that if f is nilpotent, $R_f = 0$. Additionally, if f is not nilpotent, then $f \in R_f^\times$. We can show $R_f = R[x]/(xf - 1) = R[1/f]$. We have an injection $R \subset R_f$ is R is a domain.

Example 225. Let $P \subset R$ be a prime ideal. Then $D = R \setminus P$ is a multiplicative subset. We write $D^{-1}R = R_P$. If $R = \mathbb{Z}, P = (p)$, then $\mathbb{Z}_p = \mathbb{Z}[1/p]$. On the other hand $\mathbb{Z}_P$ is the set of all rationals whose denominators are not divisible by p.

4.8 Lecture 24 (Apr 25) There will be no more homeworks because we do not have time to collect and grade it. There will be final exam review on Tuesday. The final exam will be on May 9 at 1 PM in the usual classroom.

We will consider the ideals in a localized ring. Consider ideals $I \subset R, J \subset D^{-1}R$. Denote the extension of I as ${}^eI$ and the contraction of J as ${}^cJ$.

Proposition 226.
1. *$J = {}^e({}^cJ)$;*
2. *${}^c({}^eI) = \{r \in R \mid dr \in I \text{ for some } d \in D\}$.*
3. *Prime ideals $P \subset R$ not intersecting with D are in bijection with prime ideals in $D^{-1}R$ given by extension and contraction.*
4. *If R is Noetherian then $D^{-1}R$ is Noetherian. The same holds with Noetherian replaced with Artinian.*

Why is this called localization? We consider thie geometrically.

Definition 227 (Local Ring)**.** A commutative ring with a unique maximal ideal is called a local ring.

Consider $R = k[\mathbb{A}^n]$. By the Nullstellensatz, points in $\mathbb{A}^n$ correspond exactly to maximal ideals in R. Consider R_P for P a prime ideal. Then

1. This is a local ring with unique maximal ideal ${}^eP$.
2. The prime ideals in R_P are exactly the prime ideals contained in P.

Note that the prime ideals in R_P are exactly the varieties containing Z_P, the variety cut out by P. Geometrically, R_P corresponds to the functions that do not vanish identically on Z_P. If P is maximal, then R_P sees all algebraic sets passing through the corresponding point.

4.8.1 Discrete Valuation Rings

Definition 228 (Discrete Valuation)**.** Let K be a field. A discrete valuation on K is a map $v : K^\times \to \mathbb{Z}$ satisfying:

1. v is surjective.
2. $v(xy) = v(x) + v(y)$.
3. $v(x + y) \geq \min\{v(x), v(y)\}$.

By convention, the valuation of 0 is ∞.

The valuation ring is $R = \{x \in K^\times \mid v(x) \geq 0\} \cup \{0\}$.

Example 229. Let $K = \mathbb{Q}$. We fix a prime p. We define $v_p(q) = \ell \in \mathbb{Z}$, where $q = p^\ell \frac{a}{b}$, where p does not divide a, b. The valuation is simply $\mathbb{Z}_{(p)}$.

Example 230. Consider $K = C((T))$. The valuation is the highest power of T dividing the power series, and the valuation ring is $K[[T]]$.

A valuation gives rise to a metric on K. To do this, choose a real number $\beta \in \mathbb{R}$. Assume $\beta > 1$. Then define $\|x\|_v = \beta^{-v(x)}$.

Example 231. For example, consider v_3 on $\mathbb{Q}$. Take $\beta = 3$.[39] We see that x, y are close if their difference is divisible by a large power of 3.

We can now take the completion of K with respect to this distance and we recover $\mathbb{Q}_3$, the 3-adics, which are distinct from $\mathbb{R}$, which corresponds to ∞.

Remark 232. This construction can be done for any prime p to construct the p-adics. The original valuation extends to $\mathbb{Q}_p$, and the valuation ring is $\mathbb{Z}_p$, the p-adic integers, which were constructed as a limit in the homework last semester.

Theorem 233. *The following are equivalent:*[40]

1. *R is a DVR.*
2. *R is a PID with a unique nonzero maximal ideal.*
3. *R is a UFD with a unique irreducible element T up to units.*

[39] This is the obvious choice, being the only action number in our setup. Number theorists generally do not study actual numbers.

[40] Better is R is a Noetherian locally closed domain with Krull dimension 1.

4. R is a Noetherian local domain with unique maximal ideal nonzero and principal.

5. R is a Noetherian local integrally closed domain with a unique nonzero prime ideal.

Proposition 234. *Let R be Noetherian integrally closed domain and P a minimal nonzero prime. Then R_P is a DVR.*