Algebra II

Hailey Jay

January 31, 2025

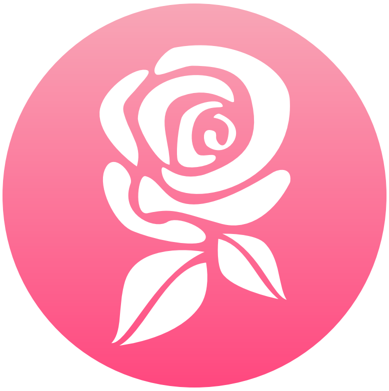


Table of Contents

Information

Time & Room	MWF 13:30-14:20, Lockett 232
Exam	Monday May 5, 10:00-12:00
Textbook	Dummit & Foote, Abstract Algebra
Professor	Ng, Richard
Office	Lockett 252
Email	rng@math.lsu.edu
Homepage	`http://www.math.lsu.edu/~rng`
Office Hours	Monday 12:30-13:20, Tuesday 13:30-1420 (Tentative)

Here's what we're going to cover:

- Chapter 13-14, Field and Galois theory;
- Chapter 15, Commutative algebra and algebras over a field;
- Chapter 10, Basics for modules and their tensor products;
- Chapter 18, Wedderburn's theorem, Maschke's theorem and linear representations of finite groups;
- POSSIBLY Chapter 17, homological algebra.

Grade Distribution

Homework	60%
Midterm	20%
Final	20%

Chapter 13

Field Theory

13.1 Extensions

Definition 13.1.1 (Field)**.** *A field is a commutative ring in which every nonzero element is invertible.*

We denote by $F^\times = F\setminus\{0\}$ the set of all invertible elements of the field F.

In general, we denote $R^\times$ as the set of all units of the ring R.

Definition 13.1.2 (Characteristic)**.** *Let F be a field with identity 1. The characteristic of F is the order of 1 in the group $(F, +)$. If the order of 1 is not finite, we define the characteristic of F to be 0.*

We denote the characteristic as $\mathrm{ch}(F)$.

We know that $\mathbb{Z}/p\mathbb{Z}$ is a field of order p if p is a prime.

Because $\mathbb{Q}$ has $n1 \neq 0$ for $n \neq 0$, $\mathrm{ch}(\mathbb{Q}) = 0$. Some other fields with characteristic zero are $\mathbb{R}, \mathbb{C}, \mathbb{C}(x) \ldots$

We denote by $\mathbb{Z}_p(x)$ as the field of rational functions over $\mathbb{Z}_p$. That is, we're adjoining the element x. It is an infinite field with finite characteristic.

Let's say that G is an abelian group. If we write it multiplicatively, $g^n = g \cdots g$ n-many times. If we write it additively, we write $g = ng$.

Proposition 13.1.3 (Characteristic of a Field)**.** *The characteristic of a field is 0 or a prime number.*

Proof. Towards a contradiction, let F be a field with $\mathrm{ch}(F) \neq 0$. Then $\mathrm{ch}(F) = nm$ for $1 < n, m < \mathrm{ch}(F)$. Because $n \cdot 1_F := n, m \cdot 1_F := m \in F$, we have that $n \cdot m = nm \cdot 1_F = 0$.

Definition 13.1.4 (Prime Subfield). *Let F be a field. The prime subfield of F is the subfield generated by* 1.

We follow with examples.

(a) $\mathbb{Z}_p(x) \geq \mathbb{Z}_p$.

(b) $\mathbb{R} > \mathbb{Q} \geq \mathbb{Q}$.

Proposition 13.1.5 (Prime Subfield). *Let F be a field and K the prime subfield of F. If $\mathrm{ch}(F) = p \neq 0$, then $K \cong \mathbb{Z}_p$. If $\mathrm{ch}(F) = 0$, $K \cong \mathbb{Q}$.*

Proof. Define $\varphi : \mathbb{Z} \to F$; $\varphi(n) = n1$. We know that φ is a ring homomorphism; I omit the proof for being rather repetetive. Such a proof is necessary to remember, however.

The kernel of φ is an ideal. In particular, because $\mathbb{Z}$ is a principal ideal domain, $\ker(\varphi) = (a)$ for some nonnegative integer a. If $a = 1$, φ is the zero map. If $a = 0$, φ is injective. In this case, $\mathbb{Z} \cong \varphi(\mathbb{Z}) \subset F$. Hence, $\mathbb{Q} \xrightarrow{\tilde{\varphi}} F$ (this is to be read $\mathbb{Q}$ extends to F), so $K \cong \mathbb{Q}$.

In the case that $a \neq 0$, then $a1 = 0$. This implies that $\mathrm{ch}(F) = p|a$. Hence $(p) \subset \ker(\varphi) = (a) \subset (p)$; Thus $(p) = (a)$. Thus, $a = p$. Hence $\varphi(\mathbb{Z}) \cong \mathbb{Z}/(p) = \mathbb{Z}_p$ by the first isomorphism theorem, so $K \cong \mathbb{Z}_p$.

Definition 13.1.6 (Extension). *If F contains a subfield K, we call F an extension of K, written as F/K.*

In this case, we have the diagram

$$\begin{array}{c} F \\ | \\ K \end{array}$$

Additionally, F is a $K-$vector space.

We denote the dimension or index of the extension $\dim_K F = [F : K]$.

For example, $\mathbb{C} \geq \mathbb{Q}$, so $\mathbb{C}$ is a $\mathbb{Q}-$linear space of uncountably infinite dimension: $[\mathbb{C} : \mathbb{Q}] = \infty$.

In a particularly obvious case, we have $[\mathbb{C} : \mathbb{R}] = 2$ for the extension $\mathbb{C}/\mathbb{R}$.

Let's take $\mathbb{Q}(i) = \{a + bi | a, b \in \mathbb{Q}\}$; $\mathbb{Q}(i)/\mathbb{Q}$ is an extension of degree 2.

Theorem 13.1.7 (Extension Index). *Let $L/K, K/F$ be finite extensions. Then L/F is finite and $[L : F] = [L : K][K : F]$.*

$$\begin{tikzcd} L \arrow[d, dash, "{[L:K]<\infty}"] \\ K \arrow[d, dash, "{[K:F]<\infty}"] \\ F \end{tikzcd}$$

In time, we learn these are tensor products.

Proof. Let $A = \{\alpha_1, \dots, \alpha_n\}$ be a basis for K over F and $B = \{\beta_1, \dots, \beta_m\}$ be a basis for L over K. Let $C = \left\{\alpha_i \beta_j \middle| i \in [n], j \in m\right\}$. Naturally, $|C| = mn$. We seek to show that C is a basis. Let $x \in L$; then $x = \sum_{i=1}^{n} k_i \beta_i$ for some $k_i \in K$. But each k_i can be written as $k_i = \sum_{j=1}^{m} f_{ij} \alpha_j$. Hence, $x = \sum_{i=1}^{n} \sum_{j=1} f_{ij} \alpha_j \beta_i$. Hence, C spans L over F.

Suppose now that $\sum f_{ij} \alpha_j b_i = 0$. Then $\sum_i \left(\sum_j f_{ij} \alpha_j\right) \beta_i = 0$. By the independence of B over K, and A over F, $f_{ij} = 0$. Thus C is independent and C is a basis.

Theorem 13.1.8 (Finite Subextension)**.** *If L/F is finite and K/F is a subextension, that is,*

$$\begin{tikzcd} L \arrow[d, dash] \\ K \arrow[d, dash] \\ F \end{tikzcd}$$

then K/F is finite and $[K : F] | [L : F]$.

A neat consequence of this is: If L/F is finite and $[L : F]$ is prime, L/F has no nontrivial subextensions.

Proposition 13.1.9 (Field to Ring Homomorphism)**.** *If $\varphi : F \to R$ is a ring homomorphism with $\varphi(1_F) \to 1_R$ where F is a field and R is a ring. Then φ is injective.*

Proof. The only ideals of F are (0) and F. As $\varphi(1) = 1$, $\ker(\varphi) =\neq F$ so $\ker \varphi = 0$ and φ is injective.

Let F be a field and $F[x]$ be a polynomial ring over F. Then, $F[x]^\times = F^\times$. Let p be irreducible in $F[x]$ and let $K = \frac{F[x]}{(p(x))}$, a field as $(p(x))$ is maximal.

Then, every element is of the form $\overline{f(x)} = f(x) + (p(x))$. Now, define $\varphi : F \to K$ via $\varphi(\alpha) = \alpha + (p(x))$. Naturally, $\varphi(1) = 1 + (p(x))$, $\varphi(\alpha+\beta) = \varphi(a)+\varphi(b)$, and $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$ so it is a ring homomorpism. Therefore, φ is an embedding and $F \cong \varphi(F)$. Identify $F \equiv \overline{F} \subset K$.

Theorem 13.1.10 (Polynomial Extension). *Let $p(x) \in F[x]$ be an irreducible polynomial. Then $p(x)$ has a root $\theta = x + (p(x)) \in K$ and $[K : F] = \deg p(x)$. Moreover, the set $\left\{1, \theta, \dots, \theta^{\deg p(x)-1}\right\}$ is a basis of K over F.*

Proof. $p(\theta) = p(x) + (p(x)) = (p(x)) = 0$ in K. We want to show that $\left\{1, \theta, \dots, \theta^{\deg p(x)-1}\right\}$ is a basis. For any $\overline{f(x)} \in K$, $\overline{f(x)} = f(x) + (p(x))$. By the division algorithm, $f(x)//p(x) = r(x)$ where $\deg r(x) < \deg p(x)$ or $r(x) = 0$. Let $r(x) = \sum_{i=0}^{n-1} a_i x^i$ for some $a_i \in F$. Moreover, $\overline{f(x)} = \overline{r(x)} = a_0\overline{1} + a_1\overline{x} + \dots a_{n-1}\overline{x}^{n-1} = \sum_{i=0}^{n-1} a_i\theta^i$ and hence $\left\{1, \theta, \dots, \theta^{\deg p(x)-1}\right\}$ spans.

Linear independence is left to the reader.

We were working on field extensions $K = \frac{F[x]}{(p(x))}$ where p is irreducible over F.

If $\theta = x + (p(x)) \in K$, then $p(\theta) = 0$. Moreover, $\left\{1, \theta, \dots, \theta^{n-1}\right\}$ spans K over F where $n = \deg p(x)$.

We want to show that $\left\{1, \theta, \dots, \theta^{n=1}\right\}$ is linearly independent over F.

Suppose $a_0 + a_1\theta + \dots + a_{n-a}\theta^{n-1} = 0$ in K.

Consider the polynomial $g(x) = a_0 + a_1 x + \dots x_{n-1}^{n-1} \in F[x]$. This implies that $g(\theta) = 0$ in K. This means that $g(x)+(p(x)) = 0$. Hence $g(x) \in (p(x))$, so $p(x)|g(x)$. This is a contradiction as $\deg p > \deg g$, unless $g \equiv 0$ and $a_0, \dots, a_{n-1} = 0$.

Therefore, $K = F[x]/(p(x))$ is an extension in which $p(x)$ has a root.

Theorem 13.1.11 (Existence of Root Extensions). *Let $f(x) \in F[x]$ be a nonconstant polynomial. There exists a field extension in which $f(x)$ has a root.*

Proof. Because $F[x]$ is a PID, we have the unique factorization $f(x) = p_1(x) \cdots p_n(x)$ for some irreducible p_i. By the preceding theorem, there exists a field K in which p_1 has a root. Therefore, $f(x)$ shares this root in K.

Theorem 13.1.12 (Existence of Root Extensions (again)). *Let $f(x) \in F[x]$ be a nonconstant polynomial. There exists a field extension in which $f(x)$ splits.*

Proof. Because $F[x]$ is a PID, we have the unique factorization $f(x) = p_1(x) \cdots p_n(x)$ for some irreducible p_i. By the preceding theorem, there exists a field K in which each p_i has a root. Iterate this process for all i to obtain the field.

For example, take the polynomial $x^2 + x + 1$ over $\mathbb{Q}$. If θ is a root, then it naturally has degree 2 so the extension field K has $[K : \mathbb{Q}] = 2$.

Let's do something concrete. We know that $\mathbb{C} \geq \mathbb{Q}$, so if we compute the roots of $p(x) = x^2 + x + 1$, we have the roots of unity of degree 3;

$$\theta = \frac{-1 \pm \sqrt{-3}}{2} = e^{\pm 2\pi i/3}.$$

It turns out that extending by either root induces isomorphic fields.

Definition 13.1.13 (Subfield Generation). *Let K/F be an extension and let $\alpha_1, \alpha_2, ... \in K$. $F(\alpha_1, ...)$ denotes the smallest subfield of K containing F and each α_i. We call this construction the subfield of K generated by F and $a_1, ...$*

We call $F(\alpha)$ a simple extension when we only extend via one element. Moreover, note that $F(\alpha_1, \alpha_2) = F(\alpha_1)(\alpha_2)$.

However, we can very bad simple extensions. Take $\mathbb{Q} \leq \mathbb{Q}(x)$, rational functions over $\mathbb{Q}$.

Let's say that α is a root of x^2+x+1 in $\mathbb{C}$. Then $\mathbb{Q}(\alpha) = \{a + b\alpha | a, b \in \mathbb{Q}\}$.

Proposition 13.1.14 (Polynomial Extension Isomorphism). *Let K be an extension of F and $\alpha \in K$ is a root of an irreducible polynomial $p(x) \in F[x]$. Then, as a field, $F[\alpha] \cong F[x]/(p(x))$.*

Proof. Define $\phi : F[x] \to K$, where $f(x) \mapsto f(\alpha)$. This is naturally a ring homomorphism; we omit the verification. Then, $\ker \phi = (g(x))$ for some $g(x) \in F[x]$. Because $p(\alpha) = 0$, $p(x) \in g(x)$. Hence, $g(x)|p(x)$. Because p is irreducible, $g(x), p(x)$ are associates and $(g(x)) = (p(x))$. Therefore, by the first isomorphism theorem, $F[x]/(p(x)) \cong \operatorname{im} \phi = F(\alpha)$ (If we were to do every single detail, we'd have to show two-way containment). Moreover, $x + (p(x)) \mapsto \alpha$.

This demonstrates that $F(\alpha)/F$ is a finite extension.

Theorem 13.1.15 (Polynomial Root Extension Isomorphism). *Let K/F be an extension and $p(x)$ be irreducible in $F[x]$. If α_1, α_2 are two roots of $p(x)$ in K, $F(\alpha_1) \cong F(\alpha_2)$ via $\alpha_1 \mapsto \alpha_2$.*

13.2 Algebraic Extensions

Definition 13.2.1 (Algebraic Extension). *K/F is called an algebraic extension if α is a root of a polynomial $f(x)$ for every $\alpha \in K$.*

If α is not algebraic, we say that α is transcendental.

For example, $\pi \in \mathbb{C}$ is transcendental over $\mathbb{Q}$, but $\sqrt{2}$ is algebraic.

A few criteria for extensions to be algebraic:

Lemma 13.2.2 (Finite Extension is Algebraic). *If K/F is finite, then K/F is algebraic.*

Proof. Interpret K as a finite dimensional vector space over F. Let $n = \deg_F K$. Let $\alpha \in K$. The set $1, \alpha, \ldots, \alpha^n$ is dependent, so there are coefficients a_k, not all 0, so that

$$a_0 + a_1\alpha + \ldots + a_k\alpha^n = 0.$$

Then α is a root of $a_0 + a_1x + \ldots + a_kx^n$.

Proposition 13.2.3 (Minimal Polynomial). *Let $\alpha \in K$ be algebraic over F. Then there exists a unique monic irreducible polynomial $m_{\alpha,F}(x)$ such that α is a root.*

Moreover, for any polynomial $f(x) \in F[x]$ such that $f(\alpha) = 0$, $m_{\alpha,F}|f(x)$ in $F[x]$.

Proof. Consider the ring homomorphism $\varphi : F[x] \to K$ defined by $\varphi(f(x)) = f(\alpha)$. The kernel is a principal ideal and hence uniquely generated by a monic polynomial $m_{\alpha,F}$. Clearly, the second statement follows as $f \in (m_{\alpha,F})$. By the first isomorphism theorem, $F[x]/(m_{\alpha,F}) \cong \varphi(F[x] \subset K)$ so it is an integral domain and hence $(m_{\alpha,F})$ is prime. Hence, $m_{\alpha,F}$ is irreducible and we are done.

Theorem 13.2.4 (Intermediate Extension Polynomial Divisibility). *Let L/F be an extension and $\alpha \in K$ be algebraic over F. Then $m_{\alpha,L}(x)|m_{\alpha,F}(x)$ in $L[x]$.*

Proof. Whence $m_{\alpha,F}(\alpha) \in L[x]$, so $m_{\alpha,L}|m_{\alpha,F}$.

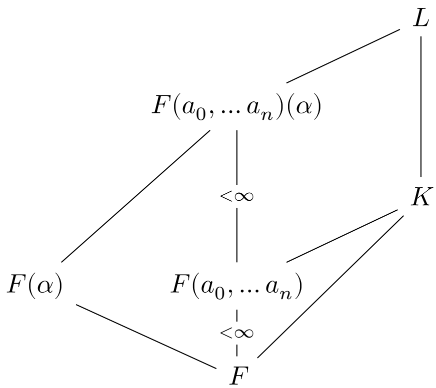
Theorem 13.2.5 (Isomorphism of Extensions). *Let $\alpha \in K$ be algebraic over F. Then $F(\alpha) \cong F[x]/(m_{\alpha,F})$ and $\{1, \alpha, \ldots, \alpha^{n+1}\}$ is a basis of $F(\alpha)$ over F, where $n = \deg(m_{\alpha,F})$*

Theorem 13.2.6 (Algebraic Subfield). *An element $\alpha \in K/F$ is algebraic over F if and only if $F(\alpha)/F$ is finite. The set $\overline{F}$ of all algebraic elements in K/F is a subfield of K.*

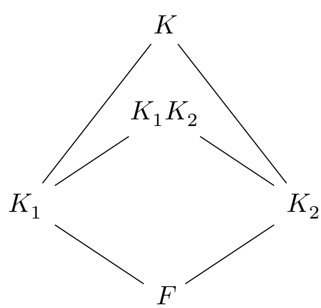
Proof. The first statement follows immediately. Let $\alpha, \beta \in K$ be algebraic over F. Then $F(\alpha, \beta)$ is finite. Thus, the sum and product of α, β are in $F(\alpha, \beta)$ and $\alpha^{-1} \in F(\alpha, \beta)$. Thus, $\overline{F}$ is a subfield.

Proposition 13.2.7 (Transitivity of Extensions)**.** *If $L/K, K/F$ are algebraic, then L/F is algebraic.*

Proof. Let $\alpha \in L$. Then α is algebraic over K, so α is a root of $a_0 + a_1 x + \dots + a_n x^n \in K[x]$. Since $[F(a_0, \dots, a_n)(\alpha) : F(a_0, \dots, a_n)] < \infty$, and each a_k is algebraic over F, $[F(a_0, \dots, a_n, \alpha) : F] < \infty$ implying that α is algebraic over F.



Definition 13.2.8 (Product Field)**.** *Let K_1, K_2 be subfields of K. We denote by K_1K_2 the subfield of K generated by K_1 and K_2.*



Proposition 13.2.9 (Product Field Properties)**.** *Let $K_1, K_2)$ be subfields of K. Suppose K_1, K_2 are finite extensions over F.*

(a) K_1K_2/F *is finite.*

(b) $[K_1K_2 : F] \leq [K_1 : F][K_2 : F]$.

(c) $\mathrm{lcm}([K_1, F], [K_2 : F]) | K_1K_2 : F$.

Proof. Let $\{\alpha_1, \dots, \alpha_n\}$ be a basis of K_1 over F and $\{\beta_1, \dots, \beta_m\}$ be a basis of K_2 over F. Then $K_1K_2 = F(\alpha_1, \dots, \alpha_n, \beta_1, \beta_n)$ and $K_1K_2 = K_1(\beta_1, \dots, \beta_m)$ implies $[K_1K_2 : K_1] \leq m$ so $[K_1K_2 : F] = [K_1K_2 : K_1][K_1][F] \leq mn$. Moreover, this final relationship implies that $[K_i : F] | [K_1K_2 : F]$ for each i, proving the final statement.

13.3 Constructibility

Definition 13.3.1 (Constructibility). *An $\alpha \in \mathbb{R}$ is called constructible if $|\alpha|$ can be constructed by straightedge and compass. We call the set of all constructible numbers $\mathbb{F}$ and assume that $\mathbb{Z} \subset \mathbb{F}$.*

Proposition 13.3.2 (Subfield of Constructible Numbers). *Let $\alpha, \beta \in \mathbb{F}$. Sums and differences are easy to construct by using a straight line through the origin, a segment of length β, and a compass of length α.*

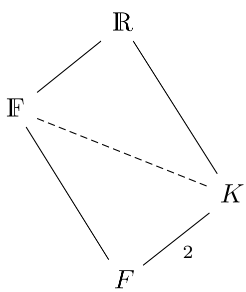
To construct products, take a triangle with one side β and foot 1, and construct a similar triangle with foot α. The corresponding side of β will have length $\alpha\beta$.

To show inverses, take a triangle of one side α and foot 1. Construct a similar triangle where the one side has length 1. The foot will have length α^{-1}.

Because $\operatorname{ch} \mathbb{F} = 0$, the prime subfield of $\mathbb{F}$ is $\mathbb{Q}$. However, as $\sqrt{2} \in \mathbb{F}$, $\mathbb{F} \supset \mathbb{Q}$.

Take $\alpha \in \mathbb{F}$. Draw a circle from $-\alpha$, 1, with centre on the x-axis. Construct a triangle to i by $-\alpha i 1$. Then, $x/1 = \alpha/x$ so $x^2 = \alpha$ and $\sqrt{\alpha} \in \mathbb{F}$.

Theorem 13.3.3 (Degree 2 Extension Closure). *Let $F \subset \mathbb{F}$ and $K \subset \mathbb{R}$ with $[K : F] = 2$. Then, $K \subset \mathbb{F}$.*



Proof. Let $\alpha \in K \backslash F$. Then α is a root of a degree 2 polynomial $p(x) = x^2 + bx + c$. Therefore, $p(x) = m_{\alpha, \mathbb{F}}(x)$. Whence $\alpha = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$ we have $F(\alpha) = F(\sqrt{b^2 - 4c})$. Because $\alpha \in \mathbb{R}$, $b^2 - 4c > 0$. However, we know already that $\sqrt{b^2 - 4c} \in \mathbb{F}$! Thus $K \subset \mathbb{F}$.

Definition 13.3.4 (Constructible Points ($\mathbb{F}^2$) in $\mathbb{R}^2$)**.** *We call $(x, y) \in \mathbb{R}^2$ constructible if $x, y \in \mathbb{F}$. Moreover, we could switch out for $x + iy \in \mathbb{C}$ if $x, y \in \mathbb{F}$. The constructible points of $\mathbb{C}$ make a field.*

We construct these points via intersections of the following objects.

(a) Straight lines through two points in $\mathbb{F}^2$;

(b) If $(h, k) \in \mathbb{F}^2$ and $r \in \mathbb{F}$, $(x - h)^2 + (y - k)^2 = r^2$.

We call $ax + by + c = 0$ an F-line if $a, b, c \in F \subset \mathbb{F}$; similarly, we infer the notion of an $\mathbb{F}$ circle.

Intersecting two F lines cannot "escape" F. A circle and line give quadratic extensions, and two circles, surprisingly, intersect on an $\mathbb{F}$−line and give also a quadratic extension. The proof requires solving the system and seeing that all of the quadratic terms cancel.

Theorem 13.3.5 (Power Two Necessity)**.** *If $\alpha \in \mathbb{R}$ is constructible, there exists an extension $\mathbb{Q} \subset K \subset \mathbb{R}$ such that $K = \mathbb{Q}(\alpha)$ $[K : \mathbb{Q}] = 2^k$ for some k.*

Proof. If α is constructible, there exists a finite sequence of constructible points (x_n, y_n) so that $\alpha \in \mathbb{Q}(x_1, y_1, \ldots, x_n, y_n)$ and $[\mathbb{Q}(x_1, \ldots, x_\ell) : \mathbb{Q}(\ldots, y_{\ell-1})] \leq 2$. Therefore $[K : \mathbb{Q}]$ is a two-power.

Theorem 13.3.6 (Trisecting the Angle)**.** *Angles, in general, cannot be trisected by compass and straightedge.*

Proof. We consider the angle $60\deg = 3\theta$. Then $(x, y) = e^{3\theta i} = \sqrt[3]{\cos\theta + i\sin\theta}^3$ is constructible. $\cos 3\theta$ is constructible, so we have that $(4\cos\theta)^3 - 3\cos\theta = 1$. Let $\alpha = \cos 3\theta$, yielding the equation $1 = 4\alpha^3 - 3\alpha$. Let $\beta = 2\alpha$. Then $0 = \beta^3 - 3\beta - 1$, an irreducible monic polynomial. Then $\mathbb{Q}(\beta) = \mathbb{Q}(\alpha)$ would be a cubic extension, a contradiction by the previous, so the angle cannot be trisected.

Theorem 13.3.7 (Doubling the Cube)**.** *A cube may not be doubled.*

Proof. If it were so, doubling the unit cube would yield sides of length $\sqrt[3]{2}$, a root of a degree three irreducible polynomial. As three divides no power of two, such a cube is not constructible.

Theorem 13.3.8 (Square with Area π)**.** *A swuare with area π cannot be constructed.*

Proof. This would mean that $\sqrt{\pi}$ would be constructible. However, $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}(\pi)] = [\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}(\pi)][\mathbb{Q}(\pi) : \mathbb{Q}] = 2\infty = \infty$ divides no power of two.

13.4 Splitting Fields

Definition 13.4.1 (Splitting Field). *Let $f(x) \in F[x]$ be a nonconstant polynomial. We call E/F a splitting field for f if f factors over E and f splits in no subfield of E.*

Theorem 13.4.2 (Roots to Splitting Field). *Let $\alpha_1, \dots, \alpha_n$ be the roots of $f(x) \in E$. Then, $F(\alpha_1, \dots, \alpha_n) \subset E$ and so we have equality.*

Example. Take $f(x) = x^3 + x + 1$ in $\mathbb{F}_2[x]$. Let α be a root of $f(x)$ in some extension $K/\mathbb{Z}_2$. Then, $f(\alpha) = 0$ and $f(\alpha^2) = (\alpha^2)^3 + \alpha^2 + 1 = (\alpha^3)^2 + \alpha^2 + 1 = (\alpha+1)^2 + \alpha^2 + 1 = 0$, so α^2 is also a root. The other root is $\alpha^2 + \alpha$.

Splitting fields for degree n polynomials have, in general, degree $n!$.

Theorem 13.4.3 (Splitting Degree). *Every polynomial $f(x) \in F[x]$ of positive degree n splits in a field of degree at most $n!$.*

Proof. It suffices to show that there is an extension K/F such that $[K/F] \leq n!$ where $f(x)$ splits. Induction. Let degree $f(x) = 1$. Then $f(x)$ splits in F. Assume that the statement holds up to some $n-1$. Let α be a root of f in some field E. We know α has degree at most n, so $f(x)/(x-\alpha)$ has degree $n-1$ in $F(\alpha)$ where $[F(\alpha) : F] \leq n$. Then, f splits in $K/F(\alpha)$, so $[K : F] = [K : F(\alpha)][F(\alpha) : F] \leq (n-1)!n = n!$.

13.4.1 Friday

Reminder: If we have a positive degree $f(x) \in F[x]$, we can always find a splitting field E/F of $f(x)$ such that $[E : F] \leq (\deg f)!$.

Lemma 13.4.4 (Isomorphism Extension). *If $\alpha \in E/F$ a root of an irreducible $f(x) \in F[x]$, then there is an isomorphism ϕ from $F \to \overline{F}$. We define $\overline{f} = \phi(f)$. Then, we may extend to an isomorphism $\tilde{\phi} : F(\alpha) \to K$ such that $\tilde{\phi}|_F = \phi$; there are exactly k such extensions, where k is the number of distinct roots of $\overline{f}$ in $\overline{E}$.*

Proof. Let $\overline{\alpha} \in \overline{E}$ be a root of $\overline{f}(x)$. Then, because $\overline{F}(\overline{\alpha}) \cong \overline{F}[x]/((\overline{f})) \cong F[x]/(f(x)) \cong F(\alpha)$

Chapter 14

Second Chapter

14.1 First Section

Appendix A

List Of Definitions

Appendix B

List Of Theorems

Temporary page!

LaTeX was unable to guess the total number of pages correctly. As there was some unprocessed data that should have been added to the final page this extra page has been added to receive it.

If you rerun the document (without altering it) this surplus page will go away, because LaTeX now knows how many pages to expect for this document.