Algebra II

Hailey Jay

February 12, 2025

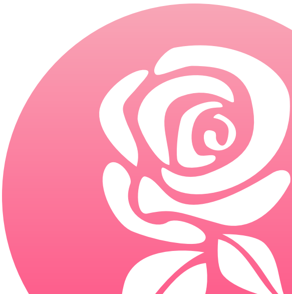


Table of Contents

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 $[L : F] = [L : K][K : F]$.*

$$\begin{array}{c} L \\ \Big| {\scriptstyle [L:K]<\infty} \\ K \\ \Big| {\scriptstyle [K:F]<\infty} \\ F \end{array}$$

In time, we learn these are tensor products.

Proof. Let $A = \{\alpha_1, \ldots, \alpha_n\}$ be a basis for K over F and $B = \{\beta_1, \ldots, \beta_m\}$ 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,*

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

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 $\{1, \theta, \dots, \theta^{\deg p(x)-1}\}$ is a basis of K over F.*

Proof. $p(\theta) = p(x) + (p(x)) = (p(x)) = 0$ in K. We want to show that $\{1, \theta, \dots, \theta^{\deg p(x)-1}\}$ 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 $\{1, \theta, \dots, \theta^{\deg p(x)-1}\}$ 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, $\{1, \theta, \dots, \theta^{n-1}\}$ spans K over F where $n = \deg p(x)$.

We want to show that $\{1, \theta, \dots, \theta^{n=1}\}$ 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 $\alpha_1, \alpha_2, \dots \in K$. $F(\alpha_1, \dots)$ denotes the smallest subfield of K containing F and each α_i. We call this construction the subfield of K generated by F and $a_1, \dots$*

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 $a_0 + a_1 x + \ldots + a_k x^n$.

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 $\{1, \alpha, \dots, \alpha^{n+1}\}$ 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.

$$\begin{tikzcd}
 & & L \arrow[dd, dash] \\
 & F(a_0, \dots a_n)(\alpha) \arrow[ur, dash] \arrow[ddl, dash] \arrow[dd, dash, "<\infty"] & \\
 & & K \arrow[dl, dash] \arrow[ddl, dash] \\
F(\alpha) \arrow[dr, dash] & F(a_0, \dots a_n) \arrow[d, dash, "<\infty"] & \\
 & F &
\end{tikzcd}$$

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.*

$$\begin{tikzcd}
 & K \arrow[ddl, dash] \arrow[ddr, dash] & \\
 & K_1K_2 \arrow[dl, dash] \arrow[dr, dash] & \\
K_1 \arrow[dr, dash] & & K_2 \arrow[dl, dash] \\
 & F &
\end{tikzcd}$$

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

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.*

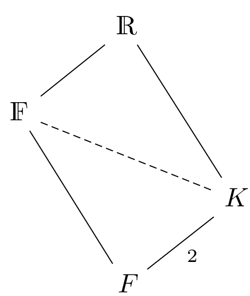
To construct products, take a triangle with one side β and foot 1, and construct a similar triangle with foot α. The corresponding side of β will have length $\alpha\beta$.

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 $\alpha \in \mathbb{Q}(x_1, y_1, \dots, x_n, y_n)$ and $[\mathbb{Q}(x_1, \dots, x_\ell) : \mathbb{Q}(\dots, y_{\ell-1})] \leq 2$. 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 $\overline{F}(\overline{\alpha}) \cong \overline{F}[x]/((\overline{f})) \cong F[x]/(f(x)) \cong F(\alpha)$, we formally have the map

$$\tilde{\phi} : F(a)\overline{\eta^{-1}} \to F[x]/(f(x))\overline{\phi} \to \overline{F}[x]/(\overline{f}(x))\overline{\overline{\eta}} \to \overline{F}(\overline{\alpha}).$$

Hence, $\phi : \alpha \mapsto \overline{\alpha}$, so the number of such extensions is the number of distinct roots $\overline{\alpha}$ of $\overline{f}(x)$

Theorem 13.4.5. *Let $\phi : a \to \overline{a}$ be an isomorphism of a field F onto $\overline{F}$. Say that $f(x) \in F[x]$ has image $\overline{f}$, and let E and $\overline{E}$ be splitting fields for the two polynomials over their respective fields. Then, ϕ can be extended to an isomorphism $\tilde{E} \to \overline{E}$. The number of such extensions is less than or equal to $[E : F]$.*

The equality holds if $\bar{f}$ has no multiple roots in $\bar{E}$.

Theorem 13.4.6 (Uniqueness of Splitting Field)**.** *The splitting field of $f(x)$ over F is unique up to isomorphism.*

Proof. Induction on $[E : F]$. If $[E : F] = 1$, then $E = F$ and f splits completely. Thus, $\bar{f}$ also splits completely so $\bar{E} = \bar{F}$. Assume $[E : F] > 1$. Then f must have a monic irreducible factor of degree greater than 1. Let $\alpha \in E$ such that $g(\alpha) = 0$. Then, $\bar{g}$ is a monic irreducible factor of $\bar{f}$, and there exists $\bar{\alpha} \in \bar{E}$ such that $\bar{g}(\bar{\alpha}) = 0$. By the preceding lemma, ϕ can be extended to $\bar{\phi} : F(\alpha) \to \bar{E}$. Let $\bar{\alpha}_1, \dots, \bar{\alpha}_\ell$ be the distinct roots of $\bar{g}$ in $\bar{E}$. Hence, there are ℓ such extensions. Then, $[E : F(\alpha)] = [E : F]/[F(\alpha) : F]$ but $[F(\alpha) : F] = \deg g(x)$. By induction, there exist at most $[E : F(\alpha)]$ possible extensions of $\tilde{\phi}$ to $\bar{\phi}$. There are at most $\ell[E : F(\alpha)] \leq \deg g(x)[E : F(\alpha)] = [E : F]$ such extensions over ϕ.

If $\bar{f}(x)$ has no multiple roots in $\bar{E}$, then $\ell = \deg \bar{g}(x)$. Then, by induction, the number of extensions is equal to $[E : F(\alpha)] \deg g(x) = [E : F]$.

Proof. [Corollary] If $\mathrm{id} : F \to F$ and $f(x) \in F$ with $E, \overline{E}$ are splitting fields of $f(x)$ over F, then the number of such extensions ϕ of id is less than or equal to $[E : F]$.[1]

Example. For $f(x) = x^3 - 2 \in \mathbb{Q}[x]$, $E = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ is the splitting field. Now, how many automorphisms do we have and what are they? Well, we have at most 6 automorphisms. We could take $\sqrt[3]{2} \mapsto \zeta_3^k \sqrt[3]{2}$, and $\zeta_3 \mapsto \bar{\zeta}_3, \zeta_3$.

13.4.2 Week 4

Last time, we learned that, if $f(x) \in F[x]$ has splitting field E and $\bar{f}(x) \in \bar{F}[x]$ has splitting field $\bar{E}$, then an isomorphism $\phi : F \to \bar{F}$ lifts to an isomorphism $\bar{\phi}$. There are at most $[E : F]$ such extensions.

$$\begin{tikzcd} E \arrow[r, "\bar{\phi}"] \arrow[d, dash] & \bar{E} \arrow[d, dash] \\ F \arrow[r, "\phi"] & \bar{F} \end{tikzcd}$$

Definition 13.4.7 (Algebraic Closure)**.** *A field $\overline{F}$ is called an algebraic closure of F if $\overline{F}/F$ is algebraic and every $f(x) \in F[x]$ splits completely.*

For an example, consider

$$\begin{tikzcd} \mathbb{C} \arrow[d, dash] \\ \bar{\mathbb{Q}} \arrow[d, dash] \\ \mathbb{Q} \end{tikzcd}$$

However, even though $\bar{\mathbb{C}} = \mathbb{C}$, $\mathbb{C}/\mathbb{Q}$ is not algebraic.

Proposition 13.4.8 (Algebraic Closure is Closed)**.** *If $\bar{F}$ is an algebraic closure of F, then $\bar{\bar{F}} = \bar{F}$.*

[1] Is this really sufficient?

Proof. Let $f(x) \in \bar{F}[x]$ be irreducible. It suffices to show that $\deg f(x) = 1$. Let $E/\bar{F}$ be the splitting field of f.

We know that $E/\bar{F}$ is finite and hence algebraic. Since $\bar{F}/F$ is algebraic, E/F° is algebraic. For any $\alpha \in E$, α is not a root of some irreducible polynomial over F. Since $\bar{F}$ is the algebraic closure of F,

$$E \subset \bar{F} \implies E = \bar{F} \implies \deg f(x) = 1.$$

Definition 13.4.9 (Separable)**.** *We call $f(x) \in F[x]$ separable if $f(x)$ has no multiple root in a splitting field E of $f(x)$ over F.*

Moreover, we say E/F is called separable if every element of E is a root of a seperable polynomial over F.

For example, $\mathbb{F}_2(t)(\sqrt{t})/\mathbb{F}_2(t)$ is inseparable.

Theorem 13.4.10. *A polynomial $f(x) \in F[x]$ has a multiple root in its splitting field over F if and only if $f(x)$ and $f'(x)$ are not relatively prime.*

Proof. Let E be a splitting field of $f(x)$ over F and $\alpha \in E$ a multiple root of $f(x)$. Then $f(x) = (x-\alpha)^m h(x)$ for some $h(x) \in F[x]$ and $m > 1$. Then $f'(x) = m(x-\alpha)^{m-1}h(x) + (x-\alpha)^m h'(x) = (x-\alpha)^{m-1}$ in $E[x]$. Let $p(x)$ be the minimal polynomial of α over F. Then $p|f, f'$.

Assume $\gcd(f(x), f'(x)) \neq 1$. Then there exists an irreducible polynomial $p(x)|f(x), f'(x)$. Let α be a root of $p(x)$ in a splitting field E of $f(x)$ over F. Then, we have that $f(\alpha) = 0 = f'(\alpha)$, so $f(x) = (x-\alpha)g(x)$ for some $g(x) \in E[x]$. Hence,

$$f'(x) = g(x) + (x-\alpha)g'(x) \implies (x-\alpha)|g(x)$$

so $(x-\alpha)^2|f(x)$ in $E[x]$, so α is a multiple root of $f(x)$. In particular, $f(x)$ is nonseperable.

Theorem 13.4.11 (Algebraic Closure)**.** *Every field F is contained in an algebraically closed field K and the set of all elements of K algebraic over F is an algebraic closure of F. Moreover, the algebraic closure of F is unique.*

Hence, if $\mathbb{F}$ is another algebraically closed field and K is all of the elements of $\mathbb{F}$ algebraic over $\mathbb{Q}$,

$$\begin{tikzcd}
\mathbb{C} \arrow[d, dash] & \mathbb{F} \arrow[d, dash] \\
\bar{\mathbb{Q}} \arrow[r, "\sim"] \arrow[d, dash] & K \arrow[dl, dash] \\
\mathbb{Q} &
\end{tikzcd}$$

13.4.3 Wednesday

Let $\mathbb{F}$ be a finite field. Let $f(x) = x^{|\mathbb{F}|} - x$ in $\mathbb{Z}_p[x]$. So, $f'(x) = -1$. Thus, the greatest common divisor of the two is 1, and f is always seperable in $\mathbb{F}$.

Additionally, for $\alpha \in \mathbb{F}^\times$, $\alpha^{|F^\times|} = 1$ so α is a root of $x^{|\mathbb{F}|-1} - 1$ and $x^{|F|-1} - 1 = \prod_{\alpha \in \mathbb{F}^\times}(x - \alpha)$. However, $x^{|\mathbb{F}|} - x = \prod_{\alpha \in \mathbb{F}}(x - \alpha)$ so. Hm!

Definition 13.4.12 (Perfect Field). *A field $\mathbb{F}$ is called perfect if every irreducible polynomial $f(x) \in F[x]$ is seperable.*

Theorem 13.4.13 (Characteristic 0 Perfection). *Every field $\mathbb{F}$ of characteristic 0 is perfect.*

Proof. Let $f(x) \in \mathbb{F}[x]$ be irreducible. Then $f'(x) \neq 0$ and $\deg f'(x) < \deg f(x)$. In particular, $f(x) \nmid f'(x)$. Since $\gcd(f(x), f'(x)) = 1, f(x)$ by irreducibility, f and f' are coprime and f is separable.

Theorem 13.4.14 (Number Fields). *Every algebraic extension over a field of characteristic 0 is separable.*

Theorem 13.4.15 (Finite Field Perfection). *Every finite field is perfect.*

Proof. Let $f(x) \in F[x]$ be irreducible and E a splitting field of f over F. In particular, E/F is finite and E is finite itself. Therefore

$x^{|E|} - x = \prod_{\alpha \in E}(x - \alpha)$ and $f(x) | x^{|E|} - x$ in $F[x]$. Therefore, $f(x)$ is a factor of a seperable polynomial and is hence separable.

Definition 13.4.16 (Frobenius Automorphism)**.** *The function x^p is called the Frobenius automorphism for fields of characteristic p.*

13.5 Cyclotomic Extensions

Let's start with $\mu_n = \left\{e^{2\pi ik/n} = \zeta_n^k | k \in [n-1]\right\}$. This is a finite group under complex multiplication. Hence, $(\mu_n, \cdot) \cong (\mathbb{Z}_n, +)$.

Definition 13.5.1 (Cyclotomic Polynomial)**.**

$$\Phi_n(x) = \prod_{\alpha \in \mu_n \text{ that are generators}} (x - \alpha)$$

is the nth cyclotomic polynomial.

We often call the generators of μ_n the primitive nth roots of unity.

13.5.1 Friday

Proposition 13.5.2 (Cyclotomic Polynomial is Monic)**.** *$\Phi_n(x)$ is a monic polynomial in $\mathbb{Z}[x]$.*

Proof. We have initially that $\Phi_n(x) \in \mathbb{C}[x]$ and $x^n - 1 \in \mathbb{Z}[x]$. We proceed by induction on n.

For our base step, $\Phi_1(x) = x - 1$. Assume now that the statement holds for any n.

Consider

$$f(x) = \prod_{d|n, n \neq d} \Phi_d(x).$$

Hence, $x^n - 1 = f(x)\Phi_n(x)$. By the division algorithm, $x^n - 1 = f(x)q(x) + r(x)$ in $\mathbb{Q}[x]$. We at least have that $f(x)|r(x) \in \mathbb{C}[x]$, meaning $r(x) = 0$. Hence, $q(x) = \Phi_n(x) \in \mathbb{Q}[x]$ so we are done by Gauss's lemma.

Theorem 13.5.3 (Irreducibility of Cyclotomic Polynomial)**.** *$\Phi_n(x)$ is irreducible in $\mathbb{Q}[x]$.*

Proof. Let α be a primitive nth root of unity. Let $g(x)$ be the minimal polynomial of α over $\mathbb{Q}$. Then $g(x)h(x) = \Phi_n(x)$ for some $h(x) \in \mathbb{Q}[x]$. By Gauss's lemma, $g(x), h(x)$ are monic in $\mathbb{Z}[x]$.

We claim that α^p is a root of $g(x)$ for any prime $p \nmid n$. Contradiction; there exists. p so that $g(\alpha^p) \neq 0$. However, $(\alpha^p)^n - 1 = 0$. By Gauss's lemma, $x^n - 1 = g(x)f(x)$ for some $f(x) \in \mathbb{Z}[x]$. Therefore $f(\alpha^p) = 0$, $f(x^p) = g(x)k(x)$, and α is a root of $f(x^p) \in \mathbb{Z}[x]$. Consider $f(x^p) \in \mathbb{Z}_p[x]$. Then $f(x^p) = f(x)^p$ and $g(x)$ has an irreducible factor dividing $f(x)$. In mod p, $x^n - 1 = g(x)f(x)$, implying that $x^n - 1$ is not separable. But if we take the derivative nx^{n-1}, it shares no factor with $x^n - 1$, implying separability, and so we have a contradiction.

By induction, $\alpha^{p_1,\dots,p_\ell}$ is a root of $g(x)$ for any primes $p_1, p_2, \dots, p_\ell \nmid n$.

Now, let θ be a primitive nth root of 1 Then $\theta = \alpha^k$ for some $k > 1, (k, n) = 1$. Hence $g(x) = \prod_{\alpha \in \mu_n \text{ primitive}} = \Theta_n(x)$ ❀

Theorem 13.5.4.

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$$

and $\mathbb{Q}(\zeta_n)$ *is the splitting field of* $x^n - 1$ *over* $\mathbb{Q}$.

We know $\Phi_p(x)$, but that is $\Phi_{p^n}(x)$? Well, it's quite simply $\Phi_p(x^{p^{n-1}})$!

What about $\Phi_{2n}(x)$ for n odd? We know that $\phi(2n) = \phi(n)$, and $-\zeta_n = \zeta_{2n}$. With a little bit of work we can show that $\Phi_{2n}(x) = \Phi_n(-x)$!

Chapter 14

Galois Theory

14.1 Automorphisms

Definition 14.1.1 (Aut(K)). *Let K be a field, and denote by* $\mathrm{Aut}(K)$ *the set of all ring automorphisms of K.*

It is endowed with a natural group structure under composition. If K/F is a field extension, define $\mathrm{Aut}(K/F) = \{\sigma \in \mathrm{Aut}(K) | \sigma(\alpha) = \alpha, \alpha \in F\}$

Because we insist $\sigma(1) = 1$, $\sigma(\alpha) = \alpha$ for $\alpha \in F$, the prime subfield of K and $\mathrm{Aut}(K) = \mathrm{Aut}(K/F)$.

These automorphism groups play nicely with composite extensions.

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

implies $\mathrm{Aut}(K/E) \leq \mathrm{Aut}(K/F)$.

Definition 14.1.2 (Invariant Subfield). *Let $G \leq \mathrm{Aut}(K/F)$. Define* $\mathrm{Inv}(G) = \{\alpha \in K | \sigma(\alpha) = \alpha \forall \sigma \in G\}$. *This is a subfield of K.*

$$\begin{array}{c} K \\ | \\ \mathrm{Inv}(G) \\ | \\ F \end{array}$$

The point of Galois theory is this: If K/F is good, there is a one to one correspondence between subextensions E/F of K/F and the subgroups of $\mathrm{Aut}(K/F)$.

Proposition 14.1.3. *(1) If* $G_1 \leq G_2 \leq \mathrm{Aut}(K/F)$*, then* $K \supset \mathrm{Inv}(G_1) \supset \mathrm{Inv}(G_1) \supset F$*.*

(2) If $F \subset E_1 \subset E_2 \subset K$*, then* $\mathrm{Aut}(K/E_1) \geq \mathrm{Aut}(K/E_2)$*.*

(3) Let $F \subset E \subset K$*. Then* $E \subset \mathrm{Inv}(\mathrm{Aut}(K/E))$*.*

(4) Let $G \leq \mathrm{Aut}(K/F)$*. Then* $G \leq \mathrm{Aut}(K/\mathrm{Inv}(G))$*.*

Proposition 14.1.4. *If* $\alpha \in K$ *is a root of an irreducible polynomial* $p(x) \in F[x]$*, then* $\sigma\alpha$ *is also a root of* $p(x)$ *for any* $\sigma \in \mathrm{Aut}(K/F)$*.*

Proof. Let $p(x) = a_0 + a_1 x + \ldots a_n x^n$ for some $a_0, \ldots, a_n \in F$. Then,

$$\begin{aligned} & 0 = p(\alpha) = a_0 + \ldots + a_n \alpha^n \\ \implies & 0 = \sigma p(\alpha) = \sigma a_0 + \ldots + \sigma a_n \sigma \alpha^n \\ \implies & 0 p(\sigma\alpha) = a_0 + \ldots + a_n (\sigma\alpha)^n. \end{aligned}$$

Theorem 14.1.5. $\mathrm{Aut}(K/F)$ *acts on the roots of any irreducible polynomial* $p(x) \in F[x]$*.*

Proposition 14.1.6. *If* K *is a splitting field for* $f(x)$ *over* F*, then* $|\mathrm{Aut}(K/F)| \leq [K : F]$*. If* $f(x)$ *has no multiple root, then we have equality.*

Proof. We have that $\sigma \in \mathrm{Aut}(K/F)$ is an extension of the identity map on F by definition. However, we know already that the number of such extensions is less than or equal to $[K : F]$ with equality when $f(x)$ has no multiple roots.

For example, let $K = \mathbb{Q}(\sqrt[3]{2})$. What is $\mathrm{Aut}(K/\mathbb{Q})$? It consists of one element; Because the three roots of $x^3 - 2 \in \mathbb{Q}[x]$ are $\sqrt[3]{2}, \sqrt[3]{2}\zeta_3, \sqrt[3]{2}\zeta_3^2$, $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$ must be the identity.

Another example. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. We already know $[K : \mathbb{Q}] = 4$. We show the data in the following diagram

$$\begin{tikzcd}
K \arrow[r, dash, "\tilde{\phi}"] \arrow[d, dash] & K \arrow[d, dash] \\
\mathbb{Q}(\sqrt{2}) \arrow[r, "\phi:\sqrt{2}\mapsto-\sqrt{2}"] \arrow[d, dash] & \mathbb{Q}(\sqrt{2}) \arrow[d, dash] \\
\mathbb{Q} \arrow[r, "\mathrm{id}"] & \mathbb{Q}
\end{tikzcd}$$

$$\tilde{\phi}_{0,0} = \mathrm{id}$$

$$\tilde{\phi}_{0,1} : \sqrt{3} \mapsto -\sqrt{3}$$

$$\tilde{\phi}_{1,0} : \sqrt{2} \mapsto -\sqrt{2}$$

$$\tilde{\phi}_{1,1} : \sqrt{3} \mapsto -\sqrt{3}, \sqrt{2} \mapsto -\sqrt{2}$$

to show that $\mathrm{Aut}(K/\mathbb{Q}) = \left\{\phi_{i,j} \middle| i, j \in \{0, 1\}\right\} \cong K_4$. The subfields are

$$\begin{tikzcd}
K \arrow[r, dash, "\tilde{\phi}"] \arrow[d, dash] & K \arrow[d, dash] \\
\mathbb{Q}(\sqrt{2}) \arrow[r, "\phi:\sqrt{2}\mapsto-\sqrt{2}"] \arrow[d, dash] & \mathbb{Q}(\sqrt{2}) \arrow[d, dash] \\
\mathbb{Q} \arrow[r, "\mathrm{id}"] & \mathbb{Q}
\end{tikzcd}$$

$$\tilde{\phi}_{0,0} = \mathrm{id}$$

$$\tilde{\phi}_{0,1} : \sqrt{3} \mapsto -\sqrt{3}$$

$$\tilde{\phi}_{1,0} : \sqrt{2} \mapsto -\sqrt{2}$$

$$\tilde{\phi}_{1,1} : \sqrt{3} \mapsto -\sqrt{3}, \sqrt{2} \mapsto -\sqrt{2}$$

Lemma 14.1.7. *Let K/F be a finite extension. Then $|\operatorname{Aut}(K/F)| < \infty$.*

Proof. Recall that this is true if K is a splitting field over F.

Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ form a basis for K over F and $p_i(x)$ a minimal polynomial for each. Let E be the splitting field of $f(x) = p_1(x)p_2(x)\ldots$ Then E is the splitting field of $f(x)$ over F. Hence,

$$|\operatorname{Aut}(K/F)| \leq |\operatorname{Aut}(E/F)| \leq [E : F].$$

Definition 14.1.8 (Galois)**.** *K/F is called Galois if $|\operatorname{Aut}(K/F)| = [K : F]$. In this case we say $\operatorname{Aut}(K/F) = \operatorname{Gal}(K/F)$*

For example, $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not galois. The automorphism group is trivial but it's of degree 3. However, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is galois!

Lemma 14.1.9 (Artin)**.** *Let $G \leq \operatorname{Aut}(K)$ be finite. Then $[K : \operatorname{Inv}(G)] \leq |G|$.*

Proof. Let $F = \operatorname{Inv}(G)$. Let $u_1, \ldots, u_n \in K$ where $m > |G|$. We want to show that this set is always dependent. Consider the system of linear equations $\sigma_i(u_1)x_1 + \ldots \sigma_i(u_m)x_m = 0$ for $i \in [n]$ and $G = \{\sigma_i\}$. More unknowns than the number of equations, we have nontrivial solutions in K! That is, there exist $b_1, \ldots, b_m \in K^m \setminus \{0\}$ which is a solution to the system.

One can assume such a solution with the least number of zero entries. Further assume that $b_1 = 1$. In particular, we have $\sigma_i(u_i) + \sigma_i(u_2)b_2 + ... \sigma_i(u_m)b_m = 0$. Apply σ_j to get

$$\sigma_j\sigma_i(u_i) + \sigma_j(\sigma_i(u_2)b_2) + ... \sigma_j(\sigma_i(u_m)b_m) = 0.$$

As i runs over all indices, we can rewrite

$$\sigma_i(u_i) + \sigma_i(u_2)\sigma_j(b_2) + ... \sigma_i(u_m)\sigma_j(b_m) = 0.$$

Hence, we have another nontrivial minimal solution. Take the difference of the two solutions, and now the first coefficient is 0. This produces another solution with at least one more 0, implying that every coefficient is zero and that $b_k \in \mathrm{Inv}(G)$. This all implies that $\{u_1, ..., u_n\}$ is $F-$linearly dependent.

Definition 14.1.10 (Character)**.** *Let G be a group and L be a field. A group homomorphism $\chi : G \to L^\times$ is a character. Well,* $\mathrm{Hom}_{Set}(G, L)$ *is an $L-$linear space.*

Let's do some examples of characters. Take $C_n = \langle g \rangle$. Let $\chi : C_n \to \mathbb{C}^\times$ by $\chi(g) = e^{2\pi k/n}$. Now let $G = GL_n(K)$. Then $\det : GL_n(K) \to K$ is a character. Last example. $\sigma \in \mathrm{Aut}(K/F)$ is a character of $K^\times$!

Theorem 14.1.11. *Let $\chi_1, ..., \chi_n$ be distinct characters of a group G valued in L. Then $\chi_1, ..., \chi_n$ are $L-$linearly independent.*

Proof. Assume to the contrary that they are linearly dependent by the coefficients b_i,

$$b_1\chi_1 + ... + b_n\chi_n = 0.$$

If $n = 1$, we're automatically fine. There exists $g_0 \in G$ such that $\chi_1(g_0) \neq g_n(g_0)$. Then, plug in gg_0 for some $g \in G$ to get

$$b_1\chi_1 gg_0 + ... + b_n\chi_n gg_0 = 0.$$

This implies

$$b_1\chi_1(g)\chi_1(g_0) + ... + b_n\chi_n(g)\chi(g_0) = 0.$$

On the other hand, $b_1\chi_1(g)\chi_n(g_0) + ... + b_n\chi_n(g)\chi_n(g_0) = 0$. Then we subtract.

$$b_1\chi_1(g_0) - b_1\chi_n(g_0) + ... + b_n\chi_n(g_0) - b_n\chi_n(g_0) = 0.$$

We could pick a maximal amount of zeros and nonzero leading coefficient for our original solution, which here would derive a contradiction.

Appendix A

List Of Definitions

Appendix B

List Of Theorems