# Algebra II

Fall 2018

## Contents

# 1 Review

**Definition 1.1.** An **ideal** $I$ in a ring $R$ is a subset of $R$ such that (i) $I$ is an additive subgroup (ii) if $x \in I$ and $r \in R$, then $rx \in I$ and $xr \in I$.

*Note:* We exclusively work in commutative rings, so we only need to check one way.

**Definition 1.2.** An ideal $P$ is **prime** if (i) $P \neq A$ (ii) if $xy \in P$ then either $x \in P$ or $y \in P$.

**Definition 1.3.** An ideal $P$ is **maximal** if it is a maximal proper ideal.

**Examples.**

- $p\mathbb{Z} \times \mathbb{Z}$ is prime and maximal in $\mathbb{Z} \times \mathbb{Z}$.
- $p\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$
- $0\mathbb{Z} \times \mathbb{Z}$ is prime but not maximal in $\mathbb{Z} \times \mathbb{Z}$.

**Proposition 1.4.** $I$ is a prime ideal if and only if $R/I$ is an ID. $I$ is a maximal ideal if and only if $R/I$ is a field.

**Corollary 1.4.1.** All maximal ideals are prime.

**Theorem 1.5 (Euclidean Algorithm).** Given $a, b \in \mathbb{Z}$ with $b > 0$, there exists unique integers $q, r$ such that $a = bq + r$ and $0 \leq r < b$. Similarly, if $f, g \in K[x]$, for some field $K$ and $g$ is a nonzero, monic polynomial, then there exist unique polynomials $q, r \in K[x]$ such that $f = gq + r$ where $0 \leq \deg(r) < \deg(q)$.

**Corollary 1.5.1.** If $f(x) \in K[x]$ is a polynomial of degree $d$ and $\alpha \in K$, then $f(\alpha) = 0$ if and only if $f(x) = (x - \alpha)q(x)$ for some $q \in K[x]$. Moreover, $f(x)$ can have at most $d$ roots in any field containing $K$.

**Theorem 1.6.** Every PID is a UFD.

*Proof.* To prove it is a factorization domain, suppose there exists a 'smallest' non-factorizable element. To get uniqueness, use induction. ■

**Proposition 1.7.** Both $K[x]$ ($K$ is a field) and $\mathbb{Z}$ are PIDs, and hence UFDs.

*Proof.* Let $I$ be an ideal in $k[x]$. If $I = (0)$, we're done. Otherwise, $I$ contains some nonzero polynomial. Choose $f(x) \in I$ to be a polynomial of minimal degree. Since $f(x) \in I$, $(f(x)) \in I$. Let $p(x) \in I$. Write

$$p(x) = q(x)f(x) + r(x),$$

where $q(x), r(x) \in k[x]$, and either $r(x) = 0$ or $\deg(r(x)) < \deg(f(x))$. Then $r(x) = p(x) - q(x)f(x)$, so $r(x) \in I$. Hence $\deg(r(x)) \geq \deg(f(x))$. Thus $r(x) = 0$, so $f(x)$ divides $p(x)$, i.e. $p(x) \in (f(x))$. *(The proof for $\mathbb{Z}$ is similar.)* ■

Recall that in an integral domain $D$, an element $\pi \in D$ is said to be irreducible if whenever $\pi = xy$, for $x, y \in D$, either $x$ or $y$ is a unit.

**Proposition 1.8.** Let $A$ be a PID. Then $\pi \in A$ is irreducible if and only if $(\pi)$ is a prime ideal.

*Proof.* For forward direction, show that $(\pi)$ is maximal. Suppose $(\pi) \subset J \subset A$, for some ideal $J$ of $A$. $A$ is a PID so $J = (x)$ for some $x \in A$. Then $\pi \in (x)$, so $\pi = xy$ for some $y \in A$. By irreducibility, either $x$ or $y$ is a unit. If $x$ is a unit, then $J = A$, if $y$ is a unit, $x = \pi y^{-1}$, so $x$ is a multiple of $\pi$, hence $J \subset (\pi)$.

For reverse, suppose $I = (a)$ is a nonzero prime ideal. Suppose $a = bc$ for $b, c \in A$. Then $bc \in (a)$, so either $b$ or $c$ is a multiple of $a$. WLOG $b = ad$ for some $d \in A$. Thus $a = bc = adc$ so $dc = 1$, hence $c$ is a unit, so $a$ is irreducible. ∎

*Thus an ideal $I$ in a PID is prime $\Leftrightarrow$ $I = (p(x))$ for irreducible $p(x) \in K[x]$ $\Leftrightarrow$ $I$ is maximal.*

**Theorem 1.9.** Let $f(x) \in K[x]$ be a *cubic* or *quadratic* polynomial. Then $f(x)$ is irreducible in $K[x]$ if and only if $f(x)$ has a root in $K$.

*Proof.* Some factor must be linear. ∎

**Proposition 1.10. (Rational Root Thorem).** Let $f(x) = a_n x^n + \ldots + a_1 x + a_0$ in $\mathbb{Z}[x]$ be primitive. If $f(x)$ has a root in $\mathbb{Q}$, that root is of the form $\frac{p}{q}$, where $(p, q) = 1$, $p | a_0$ and $q | a_n$.

*Proof.* $q^n f(\frac{p}{q}) = 0$ implies $-a_0 q^n = p(a_n p^{n-1} + \ldots + a_1 q^{n-1})$. Thus $p \mid a_0$. Similarly, $\frac{q}{p}$ is a root of $g(x) = a_n + \ldots + a_1 x^{n-1} + a_0 x^n$, so $p^n g(\frac{q}{p}) = 0$, implies $-a_n p^n = q(a_{n-1} + \ldots + a_0 q^{n-1})$. ∎

**Theorem 1.11 (Eisenstein).** Let $f(x) = a_n x^n + \ldots + a_1 x + a_0$ be in $\mathbb{Z}[x]$ and $p$ be a prime. If $p \nmid a_n$, $p | a_i$ for $1 \leq i < n$, and $p^2 \nmid a_0$, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

*Proof.* Suppose $f(x)$ is reducible over $\mathbb{Q}$. By Gauss, $f(x)$ factors over $\mathbb{Z}$. Say

$$f(x) = (b_r x^r + \ldots b_1 x + b_0)(c_s x^s + \ldots + c_1 x + c_0)$$

$b_i, c_j \in \mathbb{Z}$. Since $p \mid a_0$ and $p^2 \nmid a_0 = b_0 c_0$, $p$ divides only one of $b_0$ and $c_0$. Assume WLOG $p \mid c_0$ but $p \nmid b_0$. Note $p$ does not divide either $b_r$ or $c_s$ as $p \nmid a_n$. Let $d$ be the smallest positive integer such that $p \nmid c_d$, $1 \leq d \leq s < n$.

$$a_d = b_0 c_d + b_1 c_{d-1} + \ldots + \begin{cases} b_d c_0 & r \geq d \\ b_r c_{d-r} & \text{otherwise} \end{cases}.$$

Then $p \mid a_d$ but $p \nmid b_0 c_d$ yet $p \mid b_i c_{d-i}$ for $i < d$ (as $p \mid c_{d-i}$). ∎

**Corollary 1.11.1.** Let $p$ be a prime. Then the $p$th cyclotomic polynomial $\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + \ldots + x + 1$ is irreducible over $\mathbb{Q}$.

**Theorem 1.12.** Let $p$ be a prime and $f(x) \in \mathbb{Z}[x]$ with $\deg(f(x)) \geq 1$. Let $\overline{f(x)} \in \mathbb{Z}_p[x]$ be obtained by reducing the coefficients of $f$ modulo $p$. *We require* $\deg(\overline{f(x)}) = n$. Then $\overline{f(x)}$ is irreducible over $\mathbb{Z}_p$ implies $f(x)$ is irreducible over $\mathbb{Z}$.

*Proof.* Contrapositive. $f(x) = g(x)h(x)$ both with degree less than $n$. Reducing mod $p$, $\bar{f} = \bar{g}\bar{h}$, since $\deg f = \deg \bar{f}$, we factored $\bar{f}$ in $\mathbb{Z}_p[x]$. ∎

**Definition 1.13.** The **content** of a polynomial $p(x) = a_n x^n + \ldots + a_1 x + a_0$, is $\gcd(a_n, \ldots, a_1, a_0)$. We say $p(x)$ is **primitive** if $\text{content}(p(x)) = 1$.

**Theorem 1.14 (Gauss' Lemma 1).** $f(x) \in \mathbb{Z}[x]$ factors into a product of two polynomials of lower degrees in $\mathbb{Q}[x]$ if and only if it factors into the product to two polynomials of the same lower degrees in $\mathbb{Z}[x]$. Moreover, the polynomials from $\mathbb{Q}[x]$ and those from $\mathbb{Z}[x]$ are scalar multiples of one another. Furthermore, if $f(x)$ is primitive, then so are the polynomials $f(x)$ factors into.

*Proof.* Suffices to show for $f$ primitive. Assume $f(x) = g(x)h(x)$ in $\mathbb{Q}[x]$, where $f(x)$ is primitive. Let $a = \text{lcm}(\text{denominators of the coefficients of } g)$ and $b$ equal that of $h$. Then $abf(x) = (ag(x))(bh(x))$ where $ag(x)$ and $bh(x)$ have integer coefficients. Let $c = \text{content}(ag(x))$ and $d = \text{content}(bh(x))$. Then $ag(x) = cg_1(x)$ and $bh(x) = dh_1(x)$ where $g_1(x), h_1(x) \in \mathbb{Z}[x]$ are primitive. So

$$abf(x) = cdg_1(x)h_1(x).$$

Since $g_1(x), h_1(x)$ are primitive, so is their product. Thus $cd$ is the content of the RHS, and $ab$ is the content of the LHS. Hence $ab = cd$, and by cancellation $f(x) = g_1(x)h_1(x)$. ∎

**Theorem 1.15 (Gauss' Lemma 2).** The product of two primitive polynomials is primitive.

*Proof.* Assume $f, g$ are primitive but $f \cdot g$ is not. Then some prime $p$ divides every coefficient of $f \cdot g$. Reducing mod $p$, this implies

$$\overline{f(x)g(x)} = \overline{(f \cdot g)(x)} = 0.$$

However, neither $\overline{f(x)}$ nor $\overline{g(x)}$ is identically 0, as $f, g$ are primitive. Since $\mathbb{Z}_p[x]$ is an integral domain, we have a contradiction. ∎

# 2 Field Extensions

**Definition 2.1.** If $E$ is an extension field of $K$ (considered as a vector space), then the dimension of $E$ over $K$ is called the **degree** of $E$ over $K$ and is denoted $[E : K]$. We say the extension is *finite* if $[E : K] < \infty$.

**Definition 2.2.** An element $\alpha \in E$ is **algebraic** over $K$ us $\alpha$ is a root of some nonzero polynomial in $K[x]$. Otherwise, $\alpha$ is called **transcendental**.

**Definition 2.3.** An extension $E/K$ is **algebraic** if every $\alpha \in E$ is algebraic over $K$.

> **Examples.** Both $\sqrt[3]{5}$ and $i$ are algebraic over $\mathbb{Q}$. $\mathbb{C}$ is algebraic over $\mathbb{R}$, but not over $\mathbb{Q}$, as $\pi$ and $e$ are transcendental.

**Theorem 2.4.** Finite extensions are algebraic.

*Proof.* Suppose $[E : K] = d < \infty$. We want to show the for any $\alpha \in E$, $\alpha$ is a root of some nonzero polynomial in $K[x]$. Equivalently, we can show some non-trivial linear combination of powers of $\alpha$ is 0. Note that $\{1, \alpha, \ldots, \alpha^d\}$ is linearly dependent, so we're done. ■

**Corollary 2.4.1.** If $[E : K] = d < \infty$, then all elements of $E$ are roots of nonzero polynomials in $K[x]$ of degree at most $d$.

## 2.1 Minimal Polynomial

**Definition 2.5.** Let $E$ be an extension field of $K$. Let $\alpha \in E$ such that $\alpha$ is algebraic over $K$. The minimal polynomial of $\alpha$ over $K$, denoted $\operatorname{irr}(\alpha, K, x)$, is the monic polynomial of smallest degree in $K[x]$ with $\alpha$ as a root.

**Proposition 2.6.** Let $p(x) = \operatorname{irr}(\alpha, K, x)$. Then $p(x)$ divides all polynomials in $K[x]$ with $\alpha$ as a root. Moreover, $p(x)$ is unique.

*Proof.* Use division algorithm. ■

**Definition 2.7.** Let $E$ be an extension field of $K$. Let $\alpha \in E$ such that $\alpha$ is algebraic over $K$. Then $K[\alpha]$ is the smallest ring containing $\alpha$ and $K$, and $K(\alpha)$ is the smallest field containing $\alpha$ and $K$. Observe $K[\alpha] \subseteq K(\alpha)$.

In general, we have

$$K[a] = \{f(\alpha) : f(x) \in K[x]\}$$

and

$$K(\alpha) = \{\tfrac{f(\alpha)}{g(\alpha)} : f(x), g(x) \in K[x], g(\alpha) \neq 0\}.$$

**Theorem 2.8.** If $\alpha \in E/K$ is algebraic over $K$, then $K(\alpha) = K[\alpha]$. Moreover, if $\operatorname{irr}(\alpha, K, x)$ has degree $d$, then $\{1, \alpha, \ldots, \alpha^{d-1}\}$ forms a basis for $K[\alpha]$ over $K$. Thus $[K(\alpha) : K] = d$.

*Proof.* Recall $\phi_\alpha : K[x] \to E$ given by $f(x) \mapsto f(\alpha)$. The image of $\phi_\alpha$ is $K[a]$ and $\ker(\phi_\alpha) = (p(x))$ where $p(x) = \operatorname{irr}(\alpha, K, x)$. Then $K[x]/(p(x)) \cong K[\alpha]$, but $p(x)$ is irreducible, so $K[x]/(p(x))$ is a field. Hence $K[\alpha] = K(\alpha)$.

Suppose $\{1, \alpha, \ldots, \alpha^{d-1}\}$ weren't linearly independent, there there exists a nonzero polynomial of degree less than $d$ in $K[x]$ with $\alpha$ as a root, a contradiction. Let $\gamma \in K[\alpha]$, so

$$\gamma = a_n\alpha^n + \ldots + a_1\alpha + a_0 = f(\alpha)$$

for some $f(x) \in K[x]$. We're done if $n < d$, so suppose $n \geq d$. Let $p(x) = \text{irr}(\alpha, K, x)$. We can write

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

for $p(x), q(x), r(x) \in K[x]$ and either $r(x) = 0$ or $\deg(r(x)) < \deg(p(x))$. If $r(x) = 0$, the $\gamma = 0$, otherwise $r(x)$ is a polynomial of degree at most $d-1$, with $r(\alpha) = \gamma$. So $\gamma$ is in the span of $\{1, \alpha, \ldots, \alpha^{d-1}\}$. ■

**Theorem 2.9.** Suppose $K$ is an extension field over $E$ and $E$ is an extension field over $k$. Then $[K : k] < \infty$ if and only if $[E : k] < \infty$ and $[K : E] < \infty$. Moreover, if $K/E$ and $E/k$ are finite, then $[K : E][E : k] = [K : k]$. In particular, if $\{\alpha_i\}_{i=1}^r$ is a basis for $E$ over $k$ and $\{\beta_j\}_{j=1}^s$ is a basis for $K$ over $E$, then $\{\alpha_i\beta_j\}$ is a basis for $K$ over $k$.

*Proof.* The second statement is easy. It also shows that if $K/E$ and $E/k$ are finite extensions, then $K/k$ is a finite extension. If $K/k$ is a finite extension, then $E$ is a subspace of $K$ so $[E : k] \leq [K : k]$; any spanning set of $K$ over $k$ is also a spanning set over $E$, so $[K : E] \leq [K : k]$ ■

**Theorem 2.10.** Suppose $\alpha, \beta$ are algebraic over $k$ and that $[k(\alpha) : k] = r < \infty$ and $[k(\beta) : k] = s < \infty$. Then $k(\alpha, \beta)$ is finite over $k$ and both $r$ and $s$ divide $[k(\alpha, \beta) : k]$.

**Corollary 2.10.1.** If $r$ and $s$ are relatively prime, then $[k(\alpha, \beta) : k] = rs$.

**Corollary 2.10.2.** If $\alpha, \beta$ are algebraic over $k$, $\beta \neq 0$, then so are $\alpha + \beta, \alpha - \beta, \alpha\beta, \frac{\alpha}{\beta} \in k(\alpha, \beta)$. Moreover, all these have degree at most $rs$.

Let $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} : \alpha \text{ is algebraic over } \mathbb{Q}\}$. Then $\overline{\mathbb{Q}}$ is a field and is called the algebraic closure of $\mathbb{Q}$.

**Proposition 2.11.** If $\alpha$ is transcendental over $k$, then $k[\alpha] \cong k[x]$. *Proof.* $f(x) \mapsto f(\alpha)$.

**Theorem 2.12.** Let $L/k$ be an extension field. If $\alpha_1, \ldots, \alpha_n \in L$ are all algebraic over $k$, then $k(\alpha_1, \ldots, \alpha_n)$ is finite over $k$. *Proof.* Build tower, adjoining one $\alpha_i$ at a time.

**Theorem 2.13.** If $K/E$ and $E/k$ are extension fields, then $K/k$ is algebraic if and only if $K/E$ is algebraic and $E/k$ is algebraic.

*Proof.* ($\Rightarrow$). All $\alpha \in E$ are algebraic over $k$ ($E \subset K$); all $\alpha \in K$ are algebraic over $E$ (embed $\text{irr}(\alpha, k, x)$ in $E[x]$).

($\Leftarrow$). Let $\alpha \in K$. $\alpha$ is a root of $f(x) = b_n x^n + \ldots + b_0 \in E[x]$. Let $E_0 = k(b_0, \ldots, b_n)$. So $\alpha$ is algebraic over $E_0$. The $b_i$ are algebraic, so $E_0$ is a finitely-generated algebraic extension, thus $E_0/k$ is finite. But $E_0(\alpha)/E_0$ is finite. So $E_0(\alpha)$ is finite over $k$ and thus it is algebraic, so $\alpha$ is algebraic over $k$. ■

**Corollary 2.13.1.** If $\alpha \in E$ is a root of some polynomial with coefficients that are algebraic over $k$. Then $\alpha$ is algebraic over $k$.

**Corollary 2.13.2.** $\overline{\mathbb{Q}}$ is algebraically closed in $\mathbb{C}$.

**Theorem 2.14 (Kronecker).** Let $k$ be a field and $f(x) \in k[x]$ be a non-constant polynomial. Then there exists an extension field $E$ over $k$ in which $f(x)$ has a root.

*Proof.* Any polynomial can be factored into irreducible polynomials and any roots of an irreducible factor will be a root of $f(x)$, so it suffices to show the theorem holds in the case where $f(x)$ is irreducible. Suppose $f(x)$ is irreducible, then $(f(x))$ is maximal, thus $E = k[x]/(f(x))$ is a field. $E$ contains an isomorphic copy of $k$ (embed $k$ in $k[x]$, then mod out by $f(x)$ [why is this injective?]). Identify $k$ with its isomorphic copy in $E$, in this way $E$ as an extension field of $k$. Then $f(\bar{x}) = \overline{f(x)} = 0$, so $f$ has a root in $E$. ∎

## 2.2 Splitting Fields

**Definition 2.15.** Let $k$ be a field and $f(x) \in k[x]$, $\deg(f(x)) = n$. Then an extension $E$ of $k$ is called a splitting field of $f$ over $k$ if (1) $f(x)$ factors in to linear polynomials over $E$ and (2) this is not true for any smaller extension.

**Theorem 2.16.** Given any $f(x) \in k[x]$ of degree $n \geq 1$, there exists a splitting field for $f(x)$ over $k$. Moreover the degree of the splitting field over $k$ is at most $n!$ and if $f(x)$ is irreducible, the degree is divisible by $n$. (In fact the degree of the splitting field divides $n!$.)

**Definition 2.17.** Let $\zeta_n$ denote an $n$th primitive root of unity. The $n$th cyclotomic polynomial, w is

$$\Phi_n(x) = \prod_{(i,n)=1} (x - \zeta_n^i).$$

*Remark.* Cyclotomic polynomials are always irreducible over $\mathbb{Q}$.

**Proposition 2.18.** $f(x) \in k[x]$ has a multiple root $\alpha$ if and only if $f'(x)$ also has $\alpha$ as a root.

**Theorem 2.19.** If $f(x) \in k[x]$ is irreducible and $f(x)$ has a multiple root $\alpha$, then $f'(x)$ is identically 0.

**Theorem 2.20.** Let $k$ be a field. Let $f(x) \in k[x]$ be irreducible. Then if $\mathrm{char}(k) = 0$, $f(x)$ has no repeated roots. In characteristic $p$, $f(x)$ has repeated roots if and only if $f(x) = g_0(x^p)$ for some $g_0(x) \in k[x]$. Moreover, the multiplicity of each root of $f(x)$ is a power of $p$ and if the multiplicity is $p^s$, then $f(x) = h(x^{p^s})$ for some $h(x) \in k[x]$ having no repeated roots.

**Definition 2.21.** A separable extension is an extension $E/k$ such that for every $\alpha \in E$, the minimal polynomial of $\alpha$ over $k$ is separable (i.e. its formal derivative is nonzero).

> *Example.* Let $k = \mathbb{F}_p$. Let $z$ be an indeterminate variable over $k$ and work in $k(z)$. Let $K/k$ be the extension formed by adjoining the $p$th roots of $z$. Let $f(x) = x^p - z \in k(z)[x]$ and $\alpha$ be some root of $f(x)$. Since $\alpha$ is by definition a $p$th root of $z$, by Freshman's dream $f(x) = x^p - z = x^p - \alpha^p = (x-\alpha)^p$. Now $\mathrm{irr}(\alpha, k, x) = (x-\alpha)^d$ where $d \leq p$ (since $\alpha$ has degree at most $p$) and $d|p$, by theorem 2.17. But $d \neq 1$, if it were then there exist $f(x), g(x) \in k[x]$ so that
>
> $$\left(\frac{f(z)}{g(z)}\right)^p = z.$$
>
> Then, by Freshman's dream $f(z^p) = zg(z^p)$, which is impossible, the coefficients of $z$ on the left are congruent to 0 mod $p$, but on the right they are all congruent to 1 mod $p$. Hence $d = p$ and $f(x)$ is irreducible but has multiple roots.

**Theorem 2.22 (Primitive Element Theorem).** Let $E$ be a finite extension of degree $n$ over $k$. Suppose $E$ is separable (e.g. has characteristic 0 or finite order). Then $E = k(\alpha)$ for some

$\alpha \in E$.

*Proof.* If $k$ is finite so is $E$. Taking $\alpha$ to be a generator for the cyclic group $E^\times$ works. So assume $k$ is infinite. By induction, we may assume $n = 2$. Let $E = k(\beta, \gamma)$. Let $f(x) = \operatorname{irr}(\beta, k, x)$ and $g(x) = \operatorname{irr}(\gamma, k, x)$. Suppose $\beta = \beta_1, \beta_2, \ldots, \beta_r$ are all the roots of $f$ in $\overline{k}$ and $\gamma = \gamma_1, \ldots, \gamma_s$ are all the roots of $g$ in $\overline{k}$. There are only finitely many elements of the form

$$\frac{\beta_i - \beta}{\gamma - \gamma_j}, j \neq 1.$$

Since $k$ is infinite, there exists $a \in k$ not equal to any of the above elements. Let $\alpha = \beta + a\gamma$. Observe that $\alpha - a\gamma_j \neq \beta_i$ for all $i, j$ with $j \neq 1$. Now I claim that $k(\beta, \gamma) = k(\alpha)$. Since $\alpha \in k(\beta, \gamma)$, it suffices to show $\gamma \in k(\alpha)$.

Consider the polynomial $h(x) = f(\alpha - ax) \in k(\alpha)[x]$. Note $\gamma$ is a root of $h(x)$. Then $\operatorname{irr}(\gamma, k(\alpha), x)$ divides both $h(x)$ and $g(x)$ in $k(\alpha)[x]$. By construction, $h(x)$ and $g(x)$ have only one root in common, if they didn't then $\alpha - a\gamma_j = \beta_i$ for some $j \neq 1$, a contradiction. It follows that $\operatorname{irr}(\gamma, k(\alpha), x)$ is linear, so $\gamma \in k(\alpha)$. ■

*Example.* Let $y, z$ be two indeterminate variables over $k = \mathbb{F}_p$. Let $K$ be the extension formed by adjoining the $p$th roots of $y, z$. Let $E$ be the algebraic closure of $K$. In $E$, both $x^p - y$ and $x^p - z$ split, so there exist $a, b \in E$ such that $a^p = y$ and $b^p = z$. $K(a, b)$ is a finite extension of degree $p^2$ over $K$. Any primitive element of $K(a, b)$ must have degree $p^2$, however, for any $\gamma \in K(a, b)$, we have

$$\gamma^p = \left(\frac{f(a, b)}{g(a, b)}\right)^p = \frac{f(a^p, b^p)}{g(a^p, b^p)} \in K.$$

So $K(a, b)$ is not a primitive extension.

# 3 Galois Theory

**Definition 3.1.** An automorphism of a field $k$ is an isomorphism $k \to k$. Let $\operatorname{Aut}(k)$ denote the set of all automorphisms of a field $k$. Then $\operatorname{Gal}(K/k) = \{\sigma \in \operatorname{Aut}(k) : \sigma|_k = \mathrm{id}\}$.

**Lemma 3.2. (Into/Onto).** Suppose $K/k$ is a finite extension. Let $\sigma$ be a nonzero homomorphism from $K$ into $K$ such that $\sigma|_k = \mathrm{id}$. Then $\sigma$ is onto, so $\sigma \in \operatorname{Gal}(K/k)$.

*Proof.* View $\sigma$ as a linear map. Use rank-nullity and fact that $\sigma$ is injective whenever $\sigma \neq 0$. ■

**Fact.** Whenever $K$ is an extension field of $\mathbb{Q}$ and $r$ is an automorphism of $K$, then $\sigma|_{\mathbb{Q}} = \mathrm{id}$, so $\operatorname{Aut}(K) = \operatorname{Gal}(K/\mathbb{Q})$. The same is true of extensions of $\mathbb{F}_p$, $p$ prime.

**Proposition 3.3.**

1) $\operatorname{Aut}(k)$ forms a group under function composition.

2) $\operatorname{Gal}(K/k)$ is a subgroup of $\operatorname{Aut}(k)$.

**Definition 3.4.** If $K$ is a field and $G$ is a subgroup of $\text{Aut}(k)$, then the fixed field of $G$, denoted $K_G$, is $K_G = \{\alpha \in K : \sigma(\alpha) = \alpha \forall \sigma \in G\}$.

**Proposition 3.5.** $K_G$ is a subfield of $K$ for any subgroup $G \subset \text{Aut}(K)$. Moreover, if $H \subset \text{Gal}(K/k)$, then $K_H$ is an intermediate field.

**Examples.**

- If $K = \mathbb{C}$ and $k = \mathbb{R}$. Then if $\sigma \in \text{Gal}(K/k)$, then $\sigma(a+bi) = a+b\sigma(i)$. Since $\sigma^2(i) = -1$, we have $\sigma(i) = \pm i$. Hence the Galois group of $K/k$ consists of the identify map and the complex conjugation map. Thus $|\text{Gal}(K/k)| = 2$ and $K_{\text{Gal}(K/k)} = \mathbb{R}$.
- If $K = \mathbb{Q}(\sqrt[3]{2})$ and $k = \mathbb{Q}$. Then $\text{Gal}(K/k) = \{\text{id}\}$, since $\sigma$ is determined by its action on $\sqrt[3]{2}$, but $\sigma^3(\sqrt[3]{2}) = 2$, so there is only one choice.

**Theorem 3.6.** Suppose $[K : k] = n < \infty$. Then $|\text{Gal}(K/k)| \leq n$. In fact, if $K = k(\alpha)$ is primitive, then $|\text{Gal}(K/k)|$ is the number of distinct roots of $\text{irr}(\alpha, k, x)$ that are in $K$.

*Proof.* Observe the $\sigma$ is determined by its action on $\alpha$, as

$$\sigma(a_0 + a_1\alpha + \ldots + a_n\alpha^n) = a_0 + a_1\sigma(\alpha) + \ldots + a_n\sigma^n(\alpha),$$

for $a_i \in k$. Now, let $\alpha_1, \ldots, \alpha_d$ be the distinct roots of $f(x) = \text{irr}(\alpha, k, x)$ in $K$. Then

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

Thus there are at most $d$ choices of $\sigma(\alpha)$. Finally, for each $\alpha_i$, define $\sigma(\alpha) = \alpha_i$, and $\sigma|_k = \text{id}$. By definition,

$$\sigma(a_0 + \ldots + a_n\alpha^n) = a_0 + \ldots + a_n\alpha_i^n.$$

This is easily checked to be an onto homomorphism $K \to K$ with $\sigma|_k = \text{id}$. Moreover, to be well-defined, if $g(\alpha) = h(\alpha) \in K$, then $(g - h)(\alpha) = 0$, so $\text{irr}(\alpha, k, x)$ divides $(g - h)(x)$. Hence $\alpha_i$ are roots of $(g - h)(x)$. Thus $g(\alpha_i) = h(\alpha_i)$. ■

**Definition 3.7.** An **embedding** $\sigma$ of $K$ into $\mathbb{C}$ over $k$ is a homomorphism $\sigma : K \to \mathbb{C}$ such that $\sigma|_k = \text{id}$.

**Theorem 3.8.** Suppose $K = k(\alpha)$ is a primitive extension of degree $n$ of $k$ and $K \subset \mathbb{C}$. Let $p(x) = \text{irr}(\alpha, k, x)$ and $\alpha_i$ be all the distinct roots of $p$ is $\mathbb{C}$. Then for each $i$, there is exactly one embedding $\sigma : K \to \mathbb{C}$ over $k$ such that $\sigma(\alpha) = \alpha_i$. Moreover, these are the only embeddings.

*Proof.* Similar to 3.6. ■

## 3.1 Normal Field Extensions

**Definition 3.9.** A finite extension $K/k$ is **normal** if $K$ is the splitting field of some $f(x) \in k[x]$ over $k$.

**Lemma 3.10.** If $K/E$ is finite and $\tau$ is an embedding of $E \to \mathbb{C}$. Then there exists an embedding $\sigma : K \to \mathbb{C}$ which is an extension of $\tau$, i.e. $\sigma|_E = \tau$.

*Proof.* Similar to 3.6. ■

**Theorem 3.11.** Let $K/k$ be a finite extension. The following are equivalent:

1) $K$ is a normal extension
2) If $\alpha \in K$, then so are all the roots of $\operatorname{irr}(\alpha, k, x)$.
3) Any embedding $\sigma$ of $K$ into $\mathbb{C}$ over $k$always maps $K$ into $K$ (by the into/onto lemma, $\sigma$ maps $K$ onto $K$, thus $\sigma$ is an automorphism of $K$ fixing $k$, so $\sigma \in \operatorname{Gal}(K/k)$.)

*Proof.* $(2 \Rightarrow 1)$. Let $\alpha = \alpha_1, \ldots, \alpha_n$ be all the roots of $p(x) = \operatorname{irr}(\alpha, k, x)$. By (2), $\alpha_i \in K$, hence the s.f. of $p(x)$ over $k$ is $k(\alpha_1, \ldots, \alpha_n) = k(\alpha)$.

$(1 \Rightarrow 3)$. Let $K$ be the s.f. of $f(x) \in k[x]$ over $k$. So $K = k(\alpha_1, \ldots, \alpha_n)$, where $\alpha_i$ are all the roots of $f$ over $\mathbb{C}$. Let $\sigma$ be an embedding of $K \to \mathbb{C}$ over $k$. So $\sigma$ is a homomorphism $K \to \mathbb{C}$ such that $\sigma|_k = \mathrm{id}$. It suffices to show $\sigma$ takes $\alpha_i$ to $\alpha_j$, but $f(\sigma(\alpha_i)) = \sigma(f(\alpha_i)) = 0$.

$(3 \Rightarrow 1)$. Let $p(x)$ be an irreducible polynomial that has a root $\alpha \in K$. Let $\alpha_i$ be another root of $p(x)$ in $\mathbb{C}$ (must exist as $p(x)$ is irred). We know there exists an embedding $\tau : k(\alpha) \to k(\alpha_i)$ over $k$ with $\tau(\alpha) = \alpha_i$ (thm 3.8). Extend $\tau$ to an embedding $\sigma : K \to \mathbb{C}$ over $k$. By (3), $\sigma$ takes $K \to K$, so $\sigma(\alpha) = \alpha_i \in K$. ■

> *Example.* Let $K/E$ and $E/k$ be finite extensions. Note that $K/E$ and $E/k$ normal extensions, does not imply $K/k$ is a normal extension (take $K = k(\sqrt[4]{2}), E = k(\sqrt{2}), k = \mathbb{Q}$). Furthermore, $K/k$ normal does not imply $E/k$ is normal (it does however imply $K/E$ is a normal ext).

**Definition 3.12.** We say a finite extension $K/k$ is a **Galois extension** if it is a normal and separable extension.

**Proposition 3.13.** Let $K/k$ be a Galois extension of degree $n$ then $|\operatorname{Gal}(K/k)| = n$.

*Proof.* By primitive element theorem, $K = k(\alpha)$ for some $\alpha \in K$. By separability, $p(x) = \operatorname{irr}(\alpha, k, x)$ has no repeated roots. Let $\alpha_1, \ldots, \alpha_n$ be all the distinct roots of $p(x) \in \mathbb{C}$. By normality, these all live in $K$. The result follows by thm 3.6. ■

**Proposition 3.14.** If $K/k$ is a Galois extension. Let $G = \operatorname{Gal}(K/k)$, then $K_G = k$.

*Proof.* By definition, $k \subset K_G$. To show reverse containment, it suffices to show that for any $\alpha \in K$ with $\alpha \notin k$, we have $\alpha \notin K_G$. If $\alpha \notin k$, then $k(\alpha) \neq k$ so $\deg(\operatorname{irr}(\alpha, k, x)) > 1$. Thus there exists $\beta \in \mathbb{C}$, $\alpha \neq \beta$ that is also a root of $\operatorname{irr}(\alpha, k, x)$. There exists an embedding $\tau : k(\alpha) \to k(\beta)$ over $k$. We can extend $\tau$ to an embedding $\sigma : K \to \mathbb{C}$ over $k$. By normality, $\sigma : K \to K$ and $\sigma(\alpha) = \beta$. By into/onto, $\sigma$ is in $\operatorname{Aut}(K)$ and so $\sigma \in G$. But then $\alpha \notin K_G$. ■

## 3.2 Fundamental Theorem of Galois Theory

We say $E$ corresponds to $H \leq \mathrm{Gal}(K/k)$ if $E = K_H$ and $H = \mathrm{Gal}(K/E)$.

Let $K/k$ be a finite, Galois extension. Let $k \subset E \subset K$ be an intermediate field.

I. There is a one-to-one correspondence mapping $E \mapsto \mathrm{Gal}(K/E)$. Moreover,
   (a) If $H = \mathrm{Gal}(K/E)$, then $E = K_H$.
   (b) If $H$ be a subgroup of $G$, then $\mathrm{Gal}(K/K_H) = H$.

II. (a) Let $E$ correspond to $H$. Then $E/k$ is normal if and only if $H \triangleleft \mathrm{Gal}(K/k)$.
   (b) Let $E$ correspond to $H$. Then $E/k$ is normal if and only if $\mathrm{Gal}(E/k) \cong G/H$.

*Proof.* **Part I(a).** $K/E$ is finite, Galois. Thus by proposition 3.14, $K_H = E$.

**Part I(b).** By the primitive element theorem, $K = k(\alpha)$ for some $\alpha \in K$. Let $n = [K : K_H]$. Clearly, $H \subset \mathrm{Gal}(K/K_H)$. It suffices to show $|H| \geq n$. Let $|H| = d$ and $\sigma_1, \ldots, \sigma_d$ be the elements of $H$. Define

$$f(x) = \prod_{i=1}^{d}(x - \sigma_i(\alpha)).$$

Then $f$ has degree $d$, it has $\alpha$ as a root (as $H$ contains the identity), and $f(x) \in K_H[x]$, as for any $\tau \in H$, $f^\tau(x) = \prod(x - (\tau\sigma_i)(\alpha)) = f(x)$, i.e. the coefficient of $f$ are fixed by $H$. Therefore, $n \leq d$ as $\mathrm{irr}(\alpha, K_H, x)$ must divide $f(x)$.

**Part II(a).** $E/k$ is normal $\Leftrightarrow$ every $\sigma \in \mathrm{Gal}(K/k)$ takes $E$ to $E$ $\Leftrightarrow$ $\forall x \in E, \sigma \in G$, we have $\sigma(x) \in E$. Equivalently, $\sigma(x)$ is fixed by $H$ $\Leftrightarrow$ $\forall x \in E, \sigma \in G, \tau \in H$, $\tau\sigma(x) = \sigma(x)$ $\Leftrightarrow$ $\forall x \in E, \sigma \in G, \tau \in H$, $(\sigma^{-1}\tau\sigma)(x) = x$. This says $\sigma^{-1}\tau\sigma$ is the identity on $E$, hence it is in $\mathrm{Gal}(K/E) = H$. This is precisely what it means for $H \triangleleft \mathrm{Gal}(K/k)$.

**Part II(b).** Define $\phi : \mathrm{Gal}(K/k) \to \mathrm{Gal}(E/k)$ by $\sigma \mapsto \sigma|_E$. Since $E/k$ is normal, and $\sigma|_E$ is an embedding into $K$ over $k$, we have $\sigma|_E$ take $E$ to $E$. By into/onto, $\sigma|_E \in \mathrm{Gal}(E/k)$. Check that $\phi$ is a homomorphism. $\phi$ is onto (by normality of $E/k$, given any $\tau \in \mathrm{Gal}(E/k)$ we can extend it to $\sigma \in \mathrm{Gal}(K/k)$ and $\phi(\sigma) = \tau$). $\ker\phi$ is precisely, $\mathrm{Gal}(K/E) = H$. ∎

**Corollary 3.14.1.** If $K/k$ is finite, Galois. Let $H \leq G = \mathrm{Gal}(K/k)$ corresponds to $E$. Then $[K : K_H] = [K : E] = |H|$ and $[E : K] = [K_H : k] = [G : H]$.

*Proof.* The first statement is immediate from I(a). The second follows from $|G| = [K : k] = [K : E][E : k] = |H|[E : K]$. ∎

**Definition 3.15.** An extension $K/k$ is abelian (cyclic) if it is Galois and if $\mathrm{Gal}(K/k)$ is abelian (cyclic).

**Theorem 3.16.**

- A finite Galois extension $K/k$ of degree $n$ is cyclic if and only if there exists 1 and only 1 intermediate field of degree $d$ for each $d \mid n$.

- A finite Galois extension $K/k$ of degree $n$ is abelian if and only if there exists at least 1 intermediate field of degree $d$ for each $d \mid n$.

*Proof.* These are immediate by the correspondence between intermediate field and subgroups of $\mathrm{Gal}(K/k)$, together with the analogous statements from group theory. ■

**Corollary 3.16.1.** In a finite, abelian extension, all intermediate fields are normal. Moreover, $K/E$ and $E/k$ are also abelian. *(Any subgroup of an abelian group is normal.)*

**Corollary 3.16.2.** If $K/k$ is any finite, separable extension, then there are only finitely many intermediate fields.

*Proof.* Any such extension is contained in a finite Galois extension $L/k$ (e.g. if $K = k(\alpha)$, then let $L$ be the splitting field of $\mathrm{irr}(\alpha, k, x)$ over $k$). By the FToGT, there are finitely many intermediate fields between $L$ and $k$, and every int. field of $K/k$ is also an int. field of $L/k$. ■

**Corollary 3.16.3.** If $H_1, H_2 \leq \mathrm{Gal}(K/k)$ correspond to intermediate fields $E_1, E_2$ of $K/k$, respectively, then $H_1 \cap H_2$ corresponds to $E_1E_2$ and $\langle H_1, H_2 \rangle$ corresponds to $E_1 \cap E_2$ (Galois correspondence is order reversing).

**Definition 3.17.** We say $E_1$ and $E_2$, intermediate fields of $K/k$ (finite, Galois), are conjugate if $E_1 = k(\alpha_1)$ and $E_2 = k(\alpha_2)$, where $\alpha_1$ and $\alpha_2$ are conjugates over $k$. Equivalently, we can say there exists a $\sigma \in \mathrm{Gal}(K/k)$ that takes $\alpha_1 \mapsto \alpha_2$ and hence $\sigma(E_1) = E_2$.

**Proposition 3.18.** Conjugate intermediate fields correspond to conjugate subgroups of the Galois group. In fact, $H_1 = \sigma H_2 \sigma^{-1}$ if and only if $E_1 = \sigma(E_2)$

$$
\begin{tikzcd}[arrows=dash]
 & K = k(\sqrt[3]{2}, \zeta_3) \arrow[dl] \arrow[dr] & \\
F = k(\zeta_3) \arrow[dr, "m"'] & & E = k(\sqrt[3]{2}) \arrow[dl, "n"] \\
 & k = \mathbb{Q} &
\end{tikzcd}
$$

# 4 Insolvability of the Quintic

**Proposition 4.1.** Let $G = \mathrm{Gal}(k(\zeta_n)/k)$. Then $G$ is isomorphic to a subgroup of $\mathbb{Z}_n^*$ and in the case of $k = \mathbb{Q}$, then $G \cong \mathbb{Z}_n^*$.

*Proof.* Let $p = \mathrm{char}(k)$ and assume either $p = 0$ or $p \nmid n$. Define $\phi : G \to \mathbb{Z}_n^*$ by $\phi(\sigma) = i$ when $\sigma(\zeta_n) = \zeta_n^i$. It is easily checked that $\phi$ is an injective homomorphism. ■

**Corollary 4.1.1.** In the separable case, $k(\zeta_n)/k$ is an abelian extension. Moreover, if $\mathbb{Q} \subset E \subset \mathbb{Q}(\zeta_n)$, then $E/\mathbb{Q}$ is abelian.

**Proposition 4.2.** Let $p = \text{char}(k)$ and assume either $p = 0$ or $p \nmid n$. Suppose $\alpha$ is a root of $x^n - a$ and $\zeta_n \in k$. Then $\text{Gal}(k(\alpha)/k)$ is isomorphic to a subgroup of $\mathbb{Z}_n$. In the case where, $x^n - a$ is irreducible, it equals $\mathbb{Z}_n$.

*Proof.* Define $\phi : G \to \mathbb{Z}_n$ by $\phi(\sigma) = i$ when $\sigma(\alpha) = \zeta_n \alpha$. Check that $\phi$ is an injective homomorphism. In the case where $x^n - a$ is irreducible, the conjugates of $\alpha$ are $\{\alpha\zeta_n^i : 0 \leq i \leq n-1\}$, all of which are contained in $k(\alpha)$. ■

**Corollary 4.2.1.** $k(\alpha)$ as above is always a cyclic extension with degree dividing $n$.

**Definition 4.3.** Let $k$ be a field and $f(x) \in k[x]$. We say $f(x)$ is solvable by radicals over $k$ if its splitting field is contained in a Galois extension $E/k$ which admits a sequence of subfields $E = E_s \supset \ldots \supset E_1 \supset E_0 = k$ where $E_1 = k(\zeta_d)$ for some $d$ and for $i = 2, 3, \ldots, s$, $E_i = E_{i-1}(\alpha_i)$ where $\alpha_i$ is a root of an equation $x^{n_i} - a_i$ for some $a_i \in E_{i-1}$ and some $n_i \mid d$.

**Definition 4.4.** A group $G$ is solvable if it admits a decomposition

$$G = N_0 \rhd N_1 \rhd \ldots \rhd N_s = \{e\}$$

where $N_i/N_{i+1}$ is abelian for each $i = 0, \ldots, s-1$.

**Lemma 4.5.** If $G$ is a solvable group and $N \lhd G$, then $G/N$ is solvable.

**Theorem 4.6.** Suppose $f(x)$ is solvable by radicals over $k$. Let $K$ be the splitting field of $f(x)$ over $k$. Then $\text{Gal}(K/k)$ is solvable.

*Proof.* Let $E$ be as in definition 4.3. Let $G = \text{Gal}(E/k)$ and $N = \text{Gal}(E/K)$. It suffices to show that $G$ is solvable as $K \subset E$ and $N \lhd G$, so $\text{Gal}(K/k) \cong G/N$, which by the lemma is solvable if $G$ is solvable.

Define $N_i = \text{Gal}(E/E_i)$. In particular, note that $G = N_0$ and $\{e\} = N_s$. But $E/k$ is Galois, so $E/E_{i+1}$ is Galois and clearly, $N_{i+1} \subset N_i$. Since $N_i/N_{i+1}$ is Galois (hence normal), we have $N_{i+1} \lhd N_i$. Also $N_i/N_{i+1} \cong \text{Gal}(E_{i+1}/E_i)$ is abelian. Hence $G$ is solvable. ■

**Lemma 4.7.** Let $G^C$ denote the commutator subgroup of $G$. Then $G/N$ abelian implies $G^C \subset N$.

*Proof.* We have $\overline{xyx}^{-1}\overline{y}^{-1} = \overline{1}$ for all $\overline{x}, \overline{y} \in G/N$. Hence $xyx^{-1}y^{-1} \in N$ for all $x, y \in G$. The claim follows. ■

**Lemma 4.8.** Let $N, H$ be two subgroups of of $S_n$ $(n \geq 5)$ such that $N \lhd H$ and $H/N$ is abelian. Suppose $H$ contains all 3-cycles, then so does $N$.

*Proof.* By the lemma, we know $N$ contains all commutators of 3-cycles (as $H$ contains all 3-cycles). Choose $i, j, k, r, s$ distinct. Let $\sigma = (i, j, k)$ and $\tau = (k, r, s)$. Observe $[\sigma, \tau] = (r, k, i) \in N$, so since $i, j, k, r, s$ were arbitrary, $N$ contains all 3-cycles. ■

**Theorem 4.9.** $S_n$ is not a solvable group for all $n \geq 5$.

*Proof.* Suppose $S_n$ were solvable. Then $S_n = N_0 \triangleright \ldots \triangleright N_s = \{e\}$ and $N_i/N_{i+1}$ is abelian. By lemma 4.8, this implies that since $N_0$ contains all 3-cycles, so does $N_1$. Repeating this argument we obtain, $N_s$ contains all 3-cycles, contradiction. ■

**Proposition 4.10.** Let $q(x) \in \mathbb{Q}[x]$ be irreducible of degree $p$, prime. Suppose $q(x)$ has precisely two non-real roots. Then the Galois group of the splitting field of $q(x)$ over $\mathbb{Q}$ is isomorphic to $S_n$.

*Proof.* Let $K$ be the s.f. of $q(x)$ over $\mathbb{Q}$. Let $G = \text{Gal}(K/\mathbb{Q})$. Let $\alpha$ be a root of $q(x)$. Then $\mathbb{Q}(\alpha)$ has degree $p$ over $\mathbb{Q}$. Hence $p$ divides the order of $G$, so by Cauchy, $G$ has an element of order $p$. Identify $G$ with a subgroup $T$ of $S_p$ according to the action of the elements of $G$ on the roots of $q(x)$. We know $T$ contains a $p$-cycle (since $p$ is prime). We also know $G$ contains the complex conjugation automorphism $\tau$ (since its has exactly two non-real roots). But $\tau$ corresponds to a transposition in $T$. Hence $T$ contains a $p$-cycle and a transposition, so by group theory, $T = S_p$. ■

**Corollary 4.10.1.** Let $q(x) = 3x^5 - 15x + 5$. Let $K$ be the splitting field of $q(x)$ over $\mathbb{Q}$. Note that $q$ satisfies the conditions of proposition 4.10. So by theorem 4.9, $\text{Gal}(K/k)$ is not solvable, hence $q$ is not solvable by radicals over $\mathbb{Q}$, i.e. there is no "quintic formula".

## 4.1 Squaring the Circle, Trisecting Angles, etc.

Note all rational numbers are constructable. Furthermore, if $(x_1, y_1)$ and $(x_2, y_2)$ are the intersections of two circles, then the $x_i$ and $y_j$ all live in an at most quadratic extension of $\mathbb{Q}$. Similarly, for the intersections of a line and a circle. For example, $(x-2)^2 + (y+1)^2 = 10$ and $y = 5x - 7$ intersect at $(\frac{1}{13}(16 - \sqrt{61}), \frac{1}{13}(-11 - 5\sqrt{61}))$ and $(\frac{1}{13}(16 + \sqrt{61}), \frac{1}{13}(-11 + 5\sqrt{61}))$. Therefore, if $\alpha = (x, y)$ is any constructable pair, then both $x$ and $y$ are contained in a tower of quadratic extensions.

**Proposition 4.11.** If $\alpha = (x, y)$ is a constructable point, then $x, y$ are contained in an extension of $\mathbb{Q}$ of degree $2^k$ for some $k$.

**Corollary 4.11.1.** If $\alpha$ is transcendental over $\mathbb{Q}$ or $\alpha$ is algebraic but not a power of 2, then $\alpha$ is not constructable.

**Theorem 4.12.** It is impossible to trisect an arbitrary angle using a straight-edge and compass.

*Proof.* We can construct an angle of 60°, so if we could trisect an angles, then 20° is a constructable angle. Hence we could construct a line segment of length $\cos(20°)$. However $\cos(3x) = 4\cos^3(x) - 3\cos(x)$ so if $\alpha = \cos(20°)$, then $8\alpha^3 - 6\alpha - 1 = 0$. However, the polynomial $8x^3 - 6x - 1$ is irreducible over $\mathbb{Q}$, so $\mathbb{Q}(\alpha)$ is a degree three extension of $\mathbb{Q}$, contradiction. ■

**Theorem 4.13.** It is impossible to double a cube with a straight-edge and compass.

*Proof.* $\mathbb{Q}(\sqrt[3]{2})$ is a degree 3 extension of $\mathbb{Q}$. ■

**Theorem 4.14.** It is impossible to square a circle with a straight-edge and compass.

*Proof.* $\pi$ is transcendental over $\mathbb{Q}$, hence so is $\sqrt{\pi}$. ■

**Definition 4.15.** A Fermat prime is a prime of the form $2^m + 1$ for some non-negative integer $m$.

**Theorem 4.16.** A regular $n$-gon is constructable if and only if $n = 2^s p_1 \dots p_t$ for distinct Fermat primes $p_i$.

*Proof.* If we can construct a regular $n-gon$, then we can construct $\alpha = \cos(\frac{2\pi}{n})$. But $2\alpha = \zeta_n + \zeta_n^{-1}$, so the $n$-gon is constructable if and only if $\zeta_n + \zeta_n^{-1}$ is constructable. That is, $n$-gon constructable implies $\phi(n)/2$ is a power of 2, hence $\phi(n)$ is a power of 2. It is clear that this holds if and only if $n$ is of the above form. ∎

## 4.2 Irreducibility of Cyclotomic Polynomials

**Theorem 4.17.** $\Phi_n(x)$ is irreducible over $\mathbb{Q}$.

*Proof.* Let $\zeta = \zeta_n$ and $f(x) = \mathrm{irr}(\zeta, \mathbb{Q}, x)$. We know $f(x)$ divides $\Phi_n(x)$ since $\zeta$ is a root of $\Phi_n(x)$.

- It suffices to show that whenever $\zeta$ is a root of $f(x)$, then so is $\zeta^p$ for any $p \nmid n$. This is because we can repeat the argument to conclude $\zeta^i$ is a root of $f(x)$ for any $i$ such that $(i, n) = 1$. Hence $\Phi_n(x) \mid f(x)$, which since both polynomials are monic, implies they are equal.
- Fix a prime $p \nmid n$. We know $x^n - 1 = f(x)h(x)$ for some $h \in \mathbb{Q}[x]$. By Gauss' lemma, we can assume $f(x), h(x) \in \mathbb{Z}[x]$. Suppose $\zeta^p$ is not a root of $f(x)$. Then $\zeta^p$ must be a root of $h(x)$. Hence $f(x) \mid h(x^p)$, so $h(x^p) = f(x)g(x)$ for some $g(x) \in \mathbb{Z}[x]$. By Freshman's dream, together with Fermat's little theorem, we have $h(x^p) \equiv h(x)^p \bmod p$. So reducing modulo $p$, $\overline{h}(x)^p \equiv \overline{f}(x)\overline{g}(x)$. In particular, this implies $\overline{f}$ and $\overline{h}$ have a root in common, namely $\zeta$, a contradiction since $\overline{x^n - 1} = \overline{f}(x)\overline{h(x)}$, but $x^n - 1$ has no multiple roots in $\mathbb{F}_p$, as it has no roots in common with its derivative.

∎

## 4.3 Discriminant of a Cubic

**Definition 4.18.** For a cubic polynomial with roots $\alpha_1, \alpha_2, \alpha_3$ define

$$\delta = \alpha_1^2(\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_1 - \alpha_3)$$

and the discriminant is $\Delta = \delta^2$.

Observe that given any cubic polynomial of the form $g(x) = x^3 + ax^2 + bx + c$ we can translate it into the form $z^3 + \alpha z + \beta$ via the transformation $z = x - \frac{a}{3}$. Given a cubic of the form $f(x) = x^3 + \alpha x + \beta$, we can show that $\Delta = -4a^3 - 27b^2$.

# Appendix A - Vector Spaces

**Theorem 4.19.** Any subset $S \subset V$ that spans $V$ has a subset that is a basis. In particular, a finite-dimensional space has a finite basis.

*Proof.* If $V = \{0\}$, then $\varnothing \subset S$ is a basis for $V$. If $S$ is finite, we may remove elements from $S$ until it is linearly independent. So suppose $S$ is infinite and $V$ is finite-dimensional. Pick a nonzero vector in $S$, call it $\alpha_1$. Find another vector in $S$ not dependent on $\{\alpha_1\}$, call it $\alpha_2$. Then find a vector in $S$ not dependent on $\{\alpha_1, \alpha_2\}$. This process must terminate, since $V$ is finite-dimensional so we may not have more than $\dim V$ linearly independent vectors. Suppose we have obtained the set $\mathcal{A} = \{\alpha_1, \ldots, \alpha_n\}$, so that $S$ is linearly dependent on $\mathcal{A}$. Then $\mathcal{A}$ is a basis for $V$. ∎

**Theorem 4.20.** Any linearly independent set can be extended to form a basis (for $V$).

*Proof.* If $V$ is finite-dimensional, see above. Assume $V$ is infinite-dimensional. Let $S \subset V$ be linearly independent. Define

$$C = \{T \supset S : T \text{ is linearly independent}\}.$$

We may partially order $C$ by set inclusion. Every chain in $C$ must have an upper bound (take the union of the sets in the chain), so by Zorn's lemma, $C$ has a maximal element, $\mathcal{M}$. If $\mathcal{M}$ is not a basis for $V$, this implies there exists $x \in V$ such that $x \notin \operatorname{span}(\mathcal{M})$, hence $\mathcal{M} \cup \{x\}$ is linearly independent and contains $S$, contradiction. ∎