Algebra	Math Notes • Study Guide
	# Abstract Algebra

Table of Contents

Rings 3
Rings 3
Subrings and Ideals 4
Homomorphisms 4
Fraction Fields 5
Integers 5
Factoring 7
Factoring 7
UFDs, PIDs, and Euclidean Domains 7
Algebraic Integers 8
Quadratic Rings 8
Gaussian Integers 9
Factoring Ideals 9
Ideal Classes 10
Real Quadratic Rings 11
Polynomials 12
Polynomials 12
$\mathbb{Z}[X]$ 12
Irreducible Polynomials 13
Cyclotomic Polynomials 14
Varieties 14
Nullstellensatz 15
Fields 17
Fundamental Theorem of Algebra 17
Algebraic Elements 17
Degree of a Field Extension 17
Finite Fields 19
Modules 21
Modules 21
Structure Theorem 22
Noetherian and Artinian Rings 23
Application 1: Abelian Groups 23
Application 2: Linear Operators 24
Polynomial Rings in Several Variables 25
Tensor Products 25
Galois Theory 27
Symmetric Polynomials 27
Discriminant 27
Galois Group 27
Fixed Fields 28
Galois Extensions and Splitting Fields 28
Fundamental Theorem 29
Roots of Unity 29
Cubic Equations 30
Quartic Equations 30
Quintic Equations and the Impossibility Theorem 31

Transcendence Theory 32
Algebras 33
Division Algebras 33
References 34

1 Rings

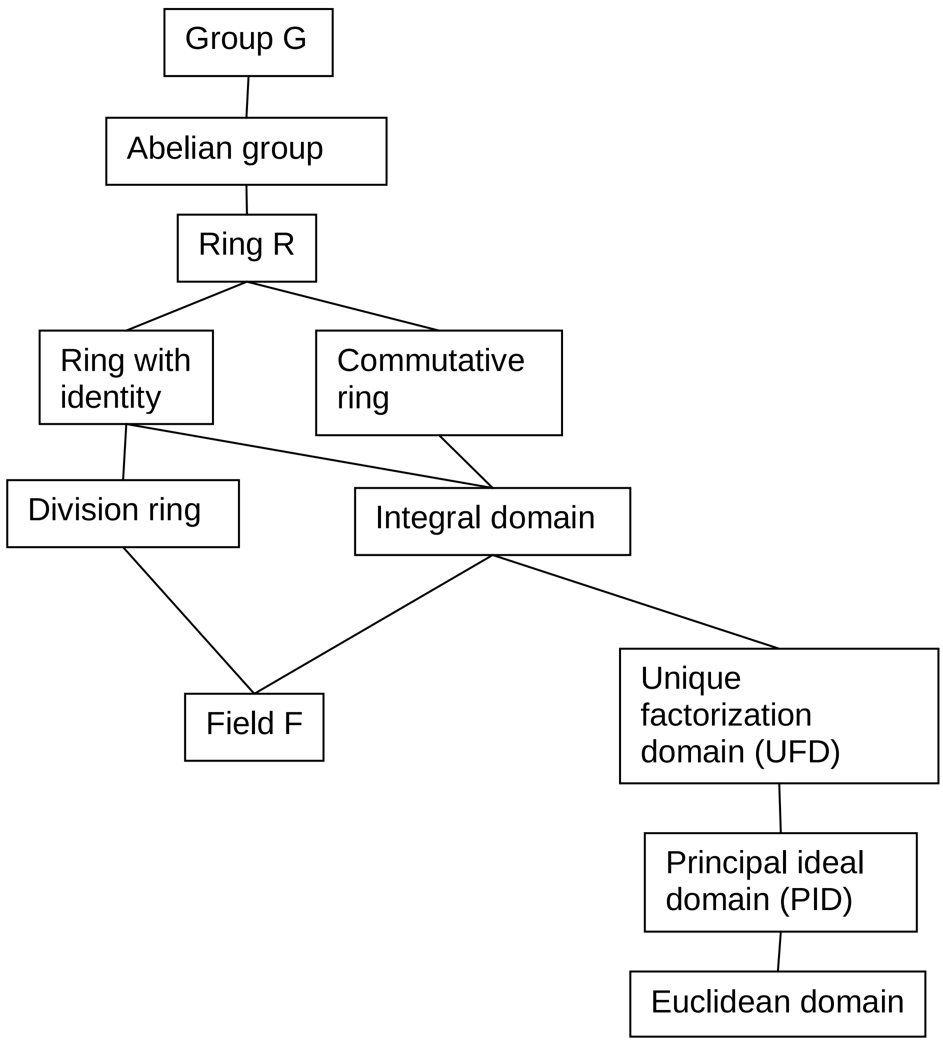
1-1 Rings

A **ring** R is a set with the operations of **addition** (+) and **multiplication** (×) satisfying:

1. R is an abelian group R_+ under addition.
2. Multiplication is associative. In a commutative ring, multiplication is commutative. A ring with identity has a multiplicative identity 1.
3. Distributive law:

$$a(b+c) = ab + ac, (a+b)c = ac + bc$$

A left/ right **zero divisor** is an element $a \in R$ so that there exists $b \neq 0$ with $ab = 0, ba = 0$, respectively. A commutative ring without zero divisors is an **integral domain**. A ring is a **division ring** if $R - \{0\}$ is a multiplicative group under multiplication (inverses exist). A division ring is a **field** if the multiplicative group is abelian.
Ex. of Rings: $\mathbb{Z}, R[x]$ (the ring of polynomials in x, where R is a ring), $R[x_1, \dots, x_n]$



Note: A field is a UFD, though not a very interesting one.

Basic properties:

1. $a0 = 0a = 0$
2. $a(-b) = (-a)b = -(ab)$
3. The multiplicative identity 1 is unique (if it exists).
4. A multiplicative inverse is unique if it exists.
5. If R is not the zero ring {0}, then $1 \neq 0$.

	6. If R is an integral domain, the cancellation law holds. Conversely, if the left (right) cancellation law holds, then R has no left (right) zero divisors. 7. A field is a division ring, and any finite integral domain is a field. From here on rings are assumed to be commutative with identity unless otherwise specified. A **unit** is an element with a multiplicative inverse. The **characteristic** of a ring is the smallest $n > 0$ so that $\underbrace{1 + \cdots + 1}_{n} = 0$. If this is never true, the characteristic is 0.
1-2	Subrings and Ideals A **subring** is a subset of a ring that is closed under addition and multiplication. An **ideal** I is a subset of a ring satisfying: 1. I is a subgroup of R_+. 2. If $s \in I, r \in R$ then $rs \in I$. Every linear combination of elements $s_i \in I$ with coefficients $r_i \in R$ is in I. The **principal ideal** $(a) = aR$ generated by a is the ideal of multiples of a. The smallest ideal generated by $a_1, \dots, a_n$ is $$(a_1, a_2, \dots, a_n) = \{r_1 a_1 + \cdots + r_n a_n \mid r_i \in R\}$$ Ideals and fields: 1. The only ideals of a field are the zero ideal and the unit ideal. 2. A ring with exactly two ideals is a field. 3. Every homomorphism from a field to a nonzero ring is injective. A **principal ideal domain (PID)** is an integral domain where every ideal is principal. Ex. $\mathbb{Z}$ is a PID. If F is a field, $F[x]$ (polynomials in x with coefficients in F) is a PID: all polynomials in the ideal are a multiple of the unique monic polynomial of lowest degree in the ideal. A **maximal ideal** of R is an ideal strictly contained in R that is not contained in any other ideal.
1-3	Homomorphisms A ring **homomorphism** $\varphi: R \to R'$ is compatible with addition and multiplication: 1. $\varphi(a + b) = \varphi(a) + \varphi(b)$ 2. $\varphi(ab) = \varphi(a)\varphi(b)$ 3. $\varphi(1) = 1$ An **isomorphism** is a bijective homomorphism and an **automorphism** is an isomorphism from R to itself. The **kernel** is $\{s \in R \mid \varphi(s) = 0\}$, and it is an ideal.
1-4	Quotient and Product Rings (11.4,6) If I is an ideal R/I is the **quotient ring**. The canonical map $\pi: R \to R/I$ sending $a \to a + I$ is a ring homomorphism that sends each element to its residue. If $I = (a_1, \dots, a_n)$, the quotient ring is obtained by "killing" the a_i, i.e. imposing the relations $a_1, \dots, a_n = 0$.

<u>Mapping Property:</u> Let $f: R \to R'$ be a ring homomorphism with kernel K and let $I \subseteq K$ be an ideal. Let $\pi: R \to R/I = \bar{R}$ be the canonical map. There is a unique homomorphism $\bar{f}: \bar{R} \to R'$ so that $\bar{f}\pi = f$.

$$\begin{tikzcd} R \arrow[rr, "f"] \arrow[dr, "\pi"'] & & R' \\ & \bar{R} = R/I \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$

<u>First Isomorphism Theorem:</u> If f is surjective and $I = K$ then $\bar{f}$ is an automorphism.
<u>Correspondence Theorem:</u> If f is surjective with kernel K,

- There is a bijective correspondence between ideals of R and ideals of R' that contain K. A subgroup of G containing K is associated with its image.
- If I corresponds to I', $R/I \cong R'/I'$.
- Corollary: Introducing relations one at a time (killing a, then $\bar{b}$) or together (killing a, b) gives the same ring. Useful in polynomial rings.

The **product ring** $R \times R'$ is the product set with componentwise addition and multiplication.

1. The additive identity is (0,0) and the multiplicative identity is (1,1).
2. The projections $\pi(x, x') = x, \pi'(x, x') = x'$ are ring homomorphisms to R, R'.
3. $(1,0), (0,1)$ are **idempotent** elements- elements such that $e^2 = 1$.

Let e be an idempotent element of a ring S.

1. $e' = 1 - e$ is idempotent, and $ee' = 0$.
2. eS is a ring (but not a subring of S unless e=1) with identity e, and multiplication by e is a ring homomorphism $S \to eS$.
3. $S \cong eS \times e'S$.

1-5 Fraction Fields

Every integral domain can be embedded as a subring of its **fraction field** F. Its elements are $\left\{\frac{a}{b} \middle| a, b \in R, b \neq 0\right\}$, where $\frac{a_1}{b_1} = \frac{a_2}{b_2} \Leftrightarrow a_1 b_2 = a_2 b_1$. Addition and multiplication are defined as in arithmetic: $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}, \frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$, and $\frac{a}{1} = a$. The field of fractions of the polynomial ring $K[x]$, K a field, is the field of **rational functions** $K(x)$.

<u>Mapping Property:</u>
Let R be an integral domain with field of fractions F, and let $\varphi: R \to F'$ be an injective homomorphism from R to a field F'. φ can be extended uniquely to an injective homomorphism $\Phi: F \to F'$ by letting $\Phi\left(\frac{a}{b}\right) = \varphi(a)\varphi(b)^{-1}$.

1-6 Integers

<u>Peano's Axioms for $\mathbb{N}$:</u>

1. $1 \in \mathbb{N}$
2. Successor function: The map $\sigma: \mathbb{N} \to \mathbb{N}$ sends an integer to the next integer $x' = \sigma(x)$; $\sigma(1) = 2, \sigma(2) = 3$ ... σ is injective, and $\sigma(n) \neq 1$ for any n (i.e. 1 is the first element).
3. Induction axiom: Let S be a subset of $\mathbb{N}$ having the following properties:
    a. $1 \in S$
    b. If $n \in S$ then $n' \in S$.

   Then $S = \mathbb{N}$. (Counting runs through all the natural numbers.)

	<u>Inductive/ Recursive Definition:</u> By induction, if an object C_1 is defined, and a rule for determining $C_{n'} = C_{n+1}$ from C_n is given, then the sequence C_k is determined uniquely. Recursive definition of… 1. Addition: $m + 1 = m'$, $m + n^{'} = (m + n)'$ (i.e. $m + (n + 1) = (m + n) + 1$) 2. Multiplication: $m \times 1 = m$, $m \times n^{'} = m \times n + m$ (i.e. $m \times (n + 1) = m \times n + m$) From these, the associative, distributive, and distributive laws can be verified. ("Peano playing") The integers can be developed from $\mathbb{N}$ by introducing an additive inverse for every element.

2 Factoring

2-1 Factoring

Vocabulary

u is a **unit**	if u has a multiplicative inverse in R	$(u) = (1)$
a **divides** b	if $b = aq$ for some $q \in R$	$(b) \subseteq (a)$
a **properly divides** b	if $b = aq$ for some $q \in R$ and neither a nor q are units	$(b) \subset (a) \subset (1)$
a and b are **relatively prime**	a and b have no common divisor except units.	$(a) \cap (b) = (1)$
a and b are **associates**	if each divides the other, or if $b = ua$, u a unit	$(a) = (b)$
a is **irreducible**	if a is not a unit and has no proper divisor (its only divisors are units and associates)	$(a) \subset (1)$, and there is no principal ideal (c) such that $(a) \subset (c) \subset (1)$.
p is a **prime element**	if p is not a unit, and whenever p divides ab, p divides a or p divides b.	$ab \in p \Rightarrow a \in (p)$ or $b \in (p)$

Ex. Nonunique factorization: $2 \cdot 3 = 6 = \left(1+\sqrt{-5}\right)\left(1-\sqrt{-5}\right)$ in $\mathbb{Z}\left[\sqrt{-5}\right]$.

2-2 UFDs, PIDs, and Euclidean Domains

A size function is a function $\sigma: R \to \mathbb{N}$. An integral domain is an **Euclidean domain** if there is a **norm** σ such that division with remainder is possible:

- For any $a, b \in R, a \neq 0$, there exist $q, r \in R$ so that $b = aq + r$, and $r = 0$ (in which case a divides b) or $\sigma(r) < \sigma(a)$.

Examples:

1. For $\mathbb{Z}$, $\sigma(a) = |a|$.
2. For $F[x]$, $\sigma(f) = \deg f$.
3. For $\mathbb{Z}[i]$, $\sigma(a) = |a|^2$.

A characterization of the GCD: Let R be a UFD. A **greatest common divisor** d of $a, b \in R$ is d such that If $e|a, b$ then $e|d$. If R is a PID, this is equivalent to $Rd = Ra + Rb$, and there exist $p, q \in R$ so $d = pa + qb$ (Bezout). a, b are relatively prime iff d is a unit.

An integral domain is a **unique factorization domain (UFD)** if factoring terminates (stopping when all elements are irreducible), and the factorization is unique up to order and multiplication by units.

The following are equivalent:

1. Factoring terminates.
2. R is **Noetherian**: it does not contain an infinite strictly increasing chain of principal ideals $(a_1) \subset (a_2) \subset \cdots$.

Class (Each includes the next)	Definition	Reasons	Properties
Ring			
Integral domain	Ring with no zero divisors		Prime element irreducible

Unique factorization domain (UFD)	Integral domain where • Factoring terminates • Factorization unique or equivalently, every irreducible element is prime.	For equivalence: If every irreducible element prime, and there are two factorizations, an element on the left divides an element on the right; they are associates and can be canceled.	Irreducible element prime GCD exists (factor and look at common prime divisors)
Principal Ideal Domain (PID)	All ideals generated by one element	A PID is a UFD: 1- Irreducible element prime: $Rd = Ra + Rb \Rightarrow$ Bezout's identity. Irreducible element prime since $p\|ab, p \nmid a \Rightarrow 1 = sp + ta \Rightarrow p\|b = spb + tab$ 2- Factoring terminates: If $(a_1) \subseteq (a_2) \subseteq \cdots$ then $\bigcup(a_i) = (b)$ is a principal ideal; $b \in (a_j)$ for some j.	Maximal ideals generated by irreducible elements
Euclidean domain	Integral domain with norm compatible with division with remainder	A Euclidean Domain is a UFD: The element of smallest size in an ideal generates it.	Euclidean algorithm works. (Given a, b, write $a = qb + r$, replace a with b, b with r.)

Ex. $\mathbb{Z}, \mathbb{Z}[i], F[x]$ are UFDs.

2-3 Algebraic Integers

An **algebraic number** is the root of an integer polynomial equation. It is an **algebraic integer** if it is the root of a monic integer polynomial equation. Equivalently, its irreducible polynomial over $\mathbb{Z}$ is monic.
A rational number is an algebraic integer iff it is an integer.

2-4 Quadratic Rings

$\mathbb{Q}[\sqrt{d}]$ is a **quadratic number field** when $d \in \mathbb{Z}$ is not a square.
The algebraic integers in $\mathbb{Q}[\delta], \delta = \sqrt{d}$, d squarefree, have the form $\alpha = a + b\delta$, where

- If $d \equiv 2,3 \pmod 4$ then a and b are integers.
- If $d \equiv 1 \pmod 4$ then a and b are both integers or half-integers ($n + \frac{1}{2}$). In other words, they have the form $a + b\eta, \eta = \frac{1}{2}(1 + \sqrt{d}); a, b \in \mathbb{Z}$.

The algebraic integers in $\mathbb{Q}[\sqrt{d}]$ form the ring of integers R in the field, $\mathbb{Z}[\delta]$ or $\mathbb{Z}[\eta]$.
Complex quadratic rings can be represented by a lattice in the complex plane.
The norm is defined by $N(z) = \bar{z}z$.

- The norm is a multiplicative function, and $N(z) = N(\bar{z})$.
- Hence $x|y \Rightarrow N(x)|N(y), x|y \Leftrightarrow N(x)|y\bar{x}$.
- An element is an unit iff its norm is 1.

If $d = -3, -2, -1, 2, 3, 5$ then R is an Euclidean domain, and hence a UFD. The only other values of d where R is a complex UFD are -7, -11, -19, -43, -67, and -163.

d	Units	Is 2 prime?
-3	$\pm 1, \pm\frac{1}{2} \pm \frac{\sqrt{3}}{2}$	Yes
-2	$1, -1$	No

-1	$\pm 1, \pm i$	No
2	Infinitely many	No
3	Infinitely many	No
5	Infinitely many	Yes

All primes in R have norm p or p^2. If the integer prime p is odd and…

- d is a perfect square modulo p, then p is the product of 2 conjugate primes of norm p.
- d is not a perfect square modulo p, then p is prime in R.

Some Theorems

1. Chinese Remainder: Given pairwise coprime b_i and any a_i, there exists a unique number $x \in R$ modulo $\prod b_i$ such that $x_i \equiv a_i (\operatorname{mod} b_i)$.
2. $R/\pi R$ has $N(\pi)$ elements. It is a field iff π is prime. (Pf. If N(π)=p then 1,…p are the distinct residues. If $N(\pi) = p^2$ then $\pi = p$; take $a + bi, 1 \le a, b \le p$. Use induction on the number of prime factors of π.)
3. Fermat's Little Theorem: $a^{N(\pi)} \equiv a (\operatorname{mod} \pi)$.
4. Euler's Theorem: $a^{\varphi(\pi)} \equiv 1 (\operatorname{mod} \pi)$.
5. Totient: $\varphi\left(\prod_{i=1}^{m} \pi_i^{a_i}\right) = N(\pi) \prod_{i=1}^{m} \frac{N(\pi_i)-1}{N(\pi_i)}$.
6. Wilson's Theorem: If π is prime, the product of all nonzero residues modulo π is congruent to -1 modulo π.
7. There are finitely many pairwise non-associated numbers with given norm.

2-5 Gaussian Integers

$\mathbb{Z}[i]$ is the ring of **Gaussian integers**.

1. If π is a Gauss prime, then $\pi\bar{\pi}$ is an integer prime or the square of an integer prime.
2. Each integer prime p is a Gauss prime or the product $\pi\bar{\pi}$ where π is a Gauss prime.
3. Primes congruent to 3 modulo 4 are Gauss primes. (They are not the sum of two squares.)
4. Primes congruent to 1 modulo 4, and 2, are the product of complex conjugate Gauss primes.

Pf. (3-4)
p is a Gauss prime iff (p) is a maximal ideal in $\mathbb{Z}[i]$, iff $\bar{R} = \mathbb{Z}[i]/(p) = \mathbb{F}_p[x]/(x^2+1)$ is a field, iff $x^2 + 1$ is irreducible (doesn't have a zero) in $\mathbb{F}_p[x]$. -1 is a square modulo p iff $p = 2$ or $p \equiv 1 \ (\operatorname{mod} 4)$.

2-6 Factoring Ideals

If A and B are ideals, then $AB = \{\sum_i a_i b_i \,|a_i \in A, b_i \in B\}$. R is the unit ideal since $AR = A$ for any R.

- Let R be a complex quadratic ring. Then $A\bar{A} = (n) = nR$ for some n; i.e. the product is a principal ideal. (Pf. Let $(a, b), (\bar{a}, \bar{b})$ be lattice bases for A, B. Let $n = \gcd(\bar{a}a, \bar{b}b, \bar{b}a + \bar{a}b)$; then $(n) \subseteq \bar{A}A$. Show n divides the four generators $\bar{a}a, \bar{b}b, \bar{b}a, \bar{a}b$, by showing $\frac{\bar{b}a}{n}, \frac{\bar{a}b}{n}$ are algebraic integers, so $\bar{A}A \subseteq (n)$.)
- Cancellation Law: Let A, B, C be nonzero ideals. $AB = AC$ iff $B = C$. $AB \subset AC \Leftrightarrow B \subset C$.
- $A|B \Leftrightarrow A \supset B$. Note that if A divides B, then *A is "larger" than B- it contains more elements; upon multiplication, many of the elements disappear.*

A **prime ideal** P satisfies any of the following equivalent conditions:

1. R/P is an integral domain.
2. $P \neq R$, and $ab \in P \Rightarrow a \in P \text{ or } b \in P$.
3. $P \neq R$, and if A, B are ideals of R, $AB \subseteq P \Rightarrow A \subseteq P \text{ or } B \subseteq P$.

Any maximal ideal is prime. If P is prime and not zero, and $P|AB$, then $P|A$ or $P|B$. Letting R be a complex quadratic ring, and B be a nonzero ideal,

1. B has finite index in R.
2. Finitely many ideals in R contain B. (Pf. Look at lattice)
3. B is in a maximal ideal.
4. B is prime iff it is maximal. (Pf. R/P is a field.)

Every proper ideal of a complex quadratic ring R factors uniquely into a product of prime ideals (up to ordering).[1]
(Pf. Use 2 and cancellation law.)
Warning: Most rings do not have unique ideal factorization since $P \supseteq B \nRightarrow P|B$.
The complex quadratic ring R is a UFD iff it is a PID. (Pf. If P is prime, P contains a prime divisor π of some element in P. Then $P = (\pi)$.)
Below, P is nonzero and prime, p is an integer prime, and π is a Gauss prime.

1. If $\bar{P}P = (n)$ then $n = p \text{ or } p^2$ for some p.
2. (p) is a prime ideal (p “remains prime”), or $p = \bar{P}P$ (p splits; if $\bar{P} = P$ then p ramifies).
3. If $d \equiv 2,3 \pmod 4$, then p generates a prime ideal iff d is not a square modulo p, iff $x^2 - d$ is irreducible in $\mathbb{F}_p[x]$. [Pf. by diagram]
4. If $d \equiv 1 \pmod 4$, then p generates a prime ideal iff $x^2 - x + \frac{1-d}{4}$ is irreducible in $\mathbb{F}_p[x]$.

Random: For nonzero ideals A, B, C, $B \supset C \Rightarrow [B{:}C] = [AB{:}AC]$. (Show for prime ideal A, split into 2 cases based on (2).)

2-7

Ideal Classes

Ideals A and B are **similar** if $B = \lambda A$ for some $\lambda \in \mathbb{C}$. (The lattices are similar and oriented the same.) Similarity classes of ideals are **ideal classes**; the ideal class of A is denoted by $\langle A \rangle$.
The class of the unit ideal $\langle R \rangle$ consists of the principal ideals.
The ideal classes form the (abelian) **class group** C of R, with $\langle A \rangle \langle B \rangle = \langle AB \rangle$. (Note $\langle A \rangle^{-1} = \langle \bar{A} \rangle$.) The class number $|C|$ tells how “badly” unique factorization of elements fails.
Measuring the size of an ideal:

- Norm: $N(A) = n$, where $(n) = \bar{A}A$. Multiplicative function.
- Index $[R{:}A]$ of A in R.
- $\Delta(A)$, the area of the parallelogram spanned by a lattice basis.
- Minimal norm of nonzero elements of A.

Relationships:

- $N(A) = [R{:}A] = \frac{\Delta(A)}{\Delta(R)}$
- If $a \in A$ has minimal nonzero norm, $N(a) \leq N(A)\mu, \mu = \begin{cases} 2\sqrt{\frac{|d|}{3}}, \text{if } d \equiv 2,3 \pmod 4 \\ \sqrt{\frac{|d|}{3}}, \text{if } d \equiv 1 \pmod 4 \end{cases}$. (Pf. $N(a) \leq \frac{2}{\sqrt{3}}\Delta(A)$)

1. Every ideal class contains an ideal A with norm $N(A) \leq \mu$. (Pf. Choose nonzero

[1] A **Dedekind domain** is a Noetherian, integrally closed integral domain with every nonzero prime ideal maximal (such as the complex quadratic rings). “Integrally closed” means that the ring contains all algebraic integers that are in its ring of fractions. Prime factorization of ideals holds in any Dedekind domain. See Algebraic Number Theory.

element with minimal norm, $(a) = AC$ for some C, $N(C) \le \mu$, $\langle C \rangle = \langle \bar{A} \rangle$,$\langle A \rangle = \langle \bar{C} \rangle$.)

2. The class group C is generated by $\langle P \rangle$, for prime ideals P with prime norm $p \le \mu$. (Pf. Factor. Either $N(P) = p$ or $P = (p)$.)
3. The class group is finite. (Pf. There are at most 2 prime ideals with norms a given integer since $A\bar{A} = (p)$ has unique factorization; use multiplicativity of norm.)

Computing the Class Group of $R = \mathbb{Z}[\sqrt{d}]$.

1. List the primes $p \le \lfloor \mu \rfloor$.
2. For each p, determine whether p splits in R by checking whether $x^2 - d$ $\big(d \equiv$ $2{,}3 \bmod 4$, $x2-x+1-d4$ $d \equiv 1 \bmod 4$ are reducible.
3. If $p = \bar{A}A$ splits in R, include $\langle A \rangle$ in the list of generators.
4. Compute the norm of some small elements (with prime divisors in the list found above), like $k + \delta. k \in \mathbb{Z}$. Factor $N(a)$ to factor $(a)(\bar{a}) = \big(N(a)\big)$; match factors using unique factorization. Note $\langle (a) \rangle = \langle (\bar{a}) \rangle = \langle R \rangle = 1$. As long as a is not divisible by one of the prime factors of $N(a)$, this amounts to replacing each prime in the factorization of $N(a)$ by one of its corresponding ideals in (3) and setting equal to 1. Repeat until there are enough relations to determine the group. [This works since if $\prod_i \langle P_i \rangle^{a_i} = 1, N(P_i) = p_i$ then there is an element $a, N(a) = \prod_i p_i^{a_i}$.]
5. For the prime 2,
   a. If $d \equiv 2{,}3 \pmod 4$, 2 ramifies: $(2) = P\bar{P}$. P has order 2 for $d \neq -1, -2$.
   b. If $d \equiv 2 \pmod 4$, $P = (2, \delta)$.
   c. If $d \equiv 3 \pmod 4), P = (2{,}1 + \delta)$.

2-8

Real Quadratic Rings

Represent $\mathbb{Z}[\sqrt{d}]$ as a lattice in the plane by associating $\alpha = a + b\sqrt{d}$ with $(u, v) = (a + b\sqrt{d}, a - b\sqrt{d})$. (The coordinates represent the two ways that $F[\delta]$ can be embedded in the real numbers, where δ is the abstract square root of d: $\delta^2 = d$.)
The norm is $N(a) = a^2 - b^2 d$ (sometimes the absolute value is used).

The units satisfy $N(a) = 1$; they lie on the hyperbola $uv = \pm 1$.
The units form an infinite group in R.
2 proofs:

1. The Pell's equation has infinitely many solutions.
2. Let Δ be the determinant for the lattice of $\mathbb{Z}[\sqrt{d}]$ and $D_s = \{(u, v) | \frac{u^2}{s^2} + s^2 v^2 \le \frac{2}{\sqrt{3}} \Delta\}$. For any lattice with determinant Δ, D_1 contains a nonzero lattice point (take the point nearest the origin and use geometry). $\varphi(x, y) = (sx, \frac{y}{s})$ is an area-preserving map; by applying φ to the lattice, we get that every D_s has a nonzero lattice point. These points have bounded norm; one norm is hit an infinite number of times. The ratios of these quadratic integers are units.

3 Polynomials

3-1 Polynomials

A **polynomial** with coefficients in R is a finite combination of nonnegative powers of the variable x. The polynomial ring over R is

$$R[X] = \left\{ \sum_{i=0}^{n} a_i x^n \,|a_i \in R \right\}$$

with X a formal variable and addition and multiplication defined by: ($f(x) = \sum_i a_i x^i$, $g(x) = \sum_i b_i x^i$)

1. $f(x) + g(x) = \sum_i (a_i + b_i) x^i$
2. $f(x)g(x) = \sum_i a_i b_j x^{i+j}$

R is a subring of R[X] when identified with the constant polynomials in R. The ring of **formal series** $R[[X]]$ is defined similarly but combinations need not be finite. Iterating, the ring of polynomials with variables $x_1, x_2, \dots, x_n$ is $R[x_1, x_2, \dots, x_n]$. (Formally, use the substitution principle below to show we can identify $R[x][y]$ with $R[x, y]$.)

Basic vocab: monomial, degree, constant, leading coefficient, monic

<u>Division with Remainder</u>: Let $f, g \in R[X]$ with the leading coefficient of f a unit. There are unique polynomials $q, r \in R[X]$ (the quotient and remainder) so that

$$g(x) = f(x)q(x) + r(x), \deg r < \deg f$$

<u>Substitution Principle</u>: Let $\varphi: R \to R'$ be a ring homomorphism. Given $a_1, \dots, a_n \in R'$, there is a unique homomorphism $\Phi: R[x_1, \dots, x_n] \to R'$ which agrees with the map φ on constant polynomials, and sends $x_i \to a_i$. For $R = R'$, this map is just substituting a_i for the variable x_i and evaluating the polynomial.

A characterization of the GCD:
The greatest common divisor d of $f, g \in R = F[x]$ is the monic polynomial defined by any of the following equivalent conditions:

1. $Rd = Rf + Rg$
2. Of all polynomials dividing f and g, d has the greatest degree.
3. If $e|f, g$ then $e|d$.

From (1), there exist $p, q \in R$ so $d = pf + qg$.

Adjoining Elements
Suppose α is an element satisfying no relation other than that implied by $f(\alpha) = 0$ where $f \in R[x]$ and has degree n. Then $R[\alpha] \cong R[x]/(f)$ is the ring extension. If f is monic, its distinct elements are the polynomials in α (with coefficients in R) of degree less than n, with $(1, \alpha, \dots, \alpha^{n-1})$ a basis. A polynomial in α is equivalent to its remainder upon division by f. R can be identified with a subring of $R[\alpha]$ as long as no constant polynomial is identified with 0.

3-2 $\mathbb{Z}[X]$

Tools for factoring in $\mathbb{Z}[X]$:

1. Inclusion in $\mathbb{Q}[X]$.
2. Reduction modulo prime p:$\psi_p: \mathbb{Z}[X] \to \mathbb{F}_p[X]$.

A polynomial in $\mathbb{Z}[X]$ is **primitive** if the greatest common divisor of its coefficients is 1, it is not constant, and the leading coefficient is positive.

Gauss's lemma: The product of primitive polynomials is primitive.
Pf. Any prime p in $\mathbb{Z}$ is prime in $\mathbb{Z}[x]$, and a prime divides a polynomial iff it divides every coefficient.

- Every nonconstant polynomial $f(x) \in \mathbb{Q}[x]$ can be written uniquely as $f(x) = cf_0(x)$, $c \in \mathbb{Q}$ and $f_0(x)$ primitive.
- If f_0 is primitive and $f_0|g \in \mathbb{Z}[x]$ in $\mathbb{Q}[x]$, then $f_0|g$ in $\mathbb{Z}[x]$. If two polynomials have a common nonconstant factor in $\mathbb{Q}[x]$, they have a common nonconstant factor in $\mathbb{Z}[x]$.
- An element of $\mathbb{Z}[x]$ is irreducible iff it is a prime integer or a primitive irreducible polynomial in $\mathbb{Q}[x]$, so every irreducible element of $\mathbb{Z}[x]$ is prime.
- Hence $\mathbb{Z}[x]$ is a UFD, and each nonzero polynomial can be written uniquely (up to ordering) as (p_i primes, q_i primitive irreducible polynomials)
$$f(x) = \pm p_1 \cdots p_m q_1(x) \cdots q_n(x)$$
- This technique can be generalized: replace $\mathbb{Z}$ with a UFD R, and $\mathbb{Q}$ with the field of fractions of R.
- By induction, if R is a UFD, then $R[x_1, \ldots, x_n]$ is a UFD.

Rational Roots Theorem: Let $f(x) = a_n x^n + \cdots + a_0, a_n \neq 0$. $-\frac{b_0}{b_1}$ (in reduced form) is a root iff $b_1 x + b_0$ divides f; if $b_1 x + b_0$ divides f then $b_1 | a_n$ and $b_0 | a_0$.

3-3

Irreducible Polynomials

The **derivative** of a polynomial is formally defined (without calculus) as
$$\left(\sum_{i=0}^{n} a_i x^i\right)' = \sum_{i=1}^{n} i a_i x^{i-1}.$$

- α is a multiple root of $f(x) \in F[x]$ iff α is a root of both $f(x)$ and $f'(x)$. α appears as a root exactly n times if $f^{(i)}(\alpha) = 0$ for $0 \le i < n$ but $f^{(n)}(\alpha) \neq 0$.
- f, f' have a common factor other than 1 iff there is a field extension where f has a multiple root.
- If f is irreducible, and $f' \neq 0$, then f has no multiple root (in any field extension). If F has characteristic 0, then f has no multiple root (in any field extension).

If $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$, $p \nmid a_n$, and the residue of f modulo p is irreducible in $\mathbb{F}_p[x]$, then f is irreducible in $\mathbb{Q}[x]$. Irreducible polynomials in $\mathbb{F}_p[x]$ can be found using the sieve method.

Eisenstein Criterion: If $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x], p \nmid a_n, p | a_{n-1}, \ldots, a_0, p^2 \nmid a_0$, then f is irreducible in $\mathbb{Q}[x]$.
Pf. Factor and take it modulo p; get $\overline{f} = (b_r x^r)(c_s x^s)$. But if $r, s \neq 0$, $p^2 | a_0$.
Extended Eisenstein's Criterion

Schönemann's Criterion: Suppose

- $k = f^n + pg, n \geq 1, p \text{ prime}, f, g \in \mathbb{Z}[x]$
- $\deg(f^n) > \deg(g)$

	• k primitive • $\overline{f}$ is irreducible in $\mathbb{F}_p[x]$ • $\bar{f} \nmid \bar{g}$. Then k is irreducible in $\mathbb{Q}[x]$. <u>Cohn's Criterion:</u> Let $b \geq 2$ and let p be a prime number. Write $p = a_n b^n + \cdots + a_1 b + a_0$ in base b. Then $f(X) = a_n X^n + \cdots + a_1 X + a_0$ is irreducible in $\mathbb{Q}[X]$. <u>Capelli's Theorem:</u> Let K be a subfield of $\mathbb{C}$ and $f, g \in K[X]$. Let a be a complex root of f and assume that f is irreducible in $K[X]$ and $g(X) - a$ is irreducible in $K[a][X]$. Then $f\big(g(X)\big)$ is irreducible in $K[X]$. [Add proof sketches.]
3-4	Cyclotomic Polynomials A **primitive nth root of unity** satisfies $\omega^n = 1$, but $\omega^m \neq 1$ for $n \in \mathbb{N}, 0 < m < n$. The nth cyclotomic polynomial is $$\Phi_n(X) = \prod_{\omega \text{ primitive } \text{ nth root}} (X - \omega).$$ The cyclotomic polynomial is an irreducible polynomial in $\mathbb{Z}[X]$ of degree $\varphi(n)$. Each polynomial $X^n - 1$ is a product of cyclotomic polynomials: $$X^n = \prod_{d\mid n} \Phi_d(X) \Rightarrow \Phi_n(X) = \frac{X^n - 1}{\prod_{d\mid n, d<n} \Phi_d(X)}$$ so $\Phi_n(X)$ has integer coefficients. *<u>Pf. of irreducibility:</u>* Lemma- if ω is a primitive nth root of unity and a zero of $f \in \mathbb{Z}[X]$ then ω^p is a root for $p \nmid n$. Proof- Suppose $\Phi_n = gh, h(\omega) = 0$, h irreducible (the minimal polynomial of ω). ω^p is also a zero of Φ_n. Suppose it is a zero of g. Then ω is a zero of $g(x^p)$, so $g(x^p) = hk$. Mod p, $g(x)^p = hk$, so g and h have a root in cogmmon, contradicting that $X^n - 1 \in \mathbb{Z}_p[X]$ has no multiple root (derivative has no common factors with $X^n - 1$). Hence ω^p is a zero of h. ■ Take powers to different primes to show that all primitive nth roots of unity divide h. Then $h = \Phi_n$ is irreducible.
3-5	Varieties 1. The set A^n of n-tuples in a field K is the **affine n-space**. 2. If S is a set of polynomials in $K[X_1, \ldots, X_n]$ then $$V(S) = \{x \in A^n \mid f(x) = 0 \text{ for all } f \in S\}$$ is a (affine) **variety**. 3. For $X \subseteq A^n$, define the **ideal** of X to be $$I(X) = \{f \in K[X_1, \ldots, X_n] \mid f \text{ vanishes on } X\}$$ Note $S \subseteq K[X_1, \ldots, X_n], X \subseteq A^n, V(S) \subseteq A^n, I(X) \subseteq K[X_1, \ldots, X_n]$. 4. The **radical** of the ideal I in a ring T is the ideal $$\sqrt{I} = \{f \in R \mid f^r \in I \text{ for some } r \in \mathbb{N}\}$$ A^n can be made into a topology (the **Zariski topology**) by taking varieties as closed sets (1-4 below).

<table>
<tr>
<td></td>
<td>
Properties:
1. $V(S) = V(I)$ where I is the ideal generated by S.
2. $\cap V(I_j) = V(\cup I_j)$
3. If $V_j = V(I_j)$ then $\bigcup_{j=1}^{r} V_j = V(\{f_1 \cdots f_r | f_j \in I_j, 1 \le j \le r\})$.
4. $A^n = V(0), \phi = V(1)$
5. $X \subseteq Y \Rightarrow I(Y) \subseteq I(X)$, $S \subseteq T \Rightarrow V(T) \subseteq V(S)$
6. $S \subseteq IV(S), X \subseteq VI(X)$
7. $VIV(S) = V(S), IVI(X) = I(X)$
8. $I(0) = K[X_1, \dots, X_n]$
9. If K is an infinite field, $I(A^n) = \{0\}$.
    a. For n=1, a nonzero polynomial only has finitely many zeros. Extend by induction.
10. $I(\{(a_1, \dots, a_n)\}) = (X_1 - a_1, \dots, X_n - a_n)$ (the ideal generated by $X_i - a_i$)
    a. Use division with remainder.
11. If $(a_1, \dots a_n) \in A^n$ then $I = (X_1 - a_1, \dots, X_n - a_n)$ is a maximal ideal.
    a. Apply the division algorithm to $f \in J \backslash I$.
12. $\sqrt{I} \subseteq IV(I)$
</td>
</tr>
<tr>
<td>3-6</td>
<td>
<h2>Nullstellensatz</h2>
<u>Hilbert Basis Theorem:</u> If R is Noetherian, then $R[x]$ is Noetherian. Thus so is $R[x_1, \dots, x_n]$. In particular, this holds for $R = \mathbb{Z}$ or a field F.
Pf. For $I \subseteq R[x]$ an ideal, the set whose elements are the leading coefficients of the polynomials in I (including 0) forms the ideal of leading coefficients in R. Take generators for this ideal and polynomials with those leading coefficients, multiplying by x as necessary so they have the same degree n. The polynomials with degree less than n form a free, Noetherian R-module P with basis $(1, x, \dots x^{n-1})$. $P \cap I$ has a finite generating set. Put the two generating sets together.
The ring of formal power series $R[[X]]$ is also Noetherian.

<u>Noether Normalization Lemma:</u> Let A be a finitely generated K-algebra. There exists a subset $\{y_1, \dots, y_r\}$ of A such that the y_i are algebraically independent over K and A is integral over $K[y_1, \dots, y_r]$ (all elements of A are algebraic integers over $K[y_1, \dots, y_r]$).
<u>Pf.</u> Induct on n; n=1 trivial. Take a maximally algebraically independent subset $\{x_1, \dots, x_r\} \subseteq \{x_1, \dots, x_n\}$; assume $n > r$. By algebraic dependency, there exists $f \in K[X_1, \dots, X_n]$ so that $f(x_1, \dots, x_n) = 0$. Lexicographically order the monomials, and choose weights w_i to match the lexicographic order. Set $x_i = z_i + x_n^{w_i}$. Then we get a polynomial in x_n, where term with the highest power of x_n is uncancelled. x_n is integral over $K[z_1, \dots, z_{n-1}]$; finish by induction.
<u>Cor.</u> If B is a finitely generated K-algebra, and I is a maximal ideal, then B/I is a finite extension of K (K is embedded via $c \rightsquigarrow c + I$.): In the above, we must have $r = 0$; B/I is algebraic over K.

<u>Hilbert's Nullstellensatz:</u> For any field K and $n \in \mathbb{N}$, the following are equivalent:
1. K is algebraically closed.
2. (Maximal Ideal Theorem) The maximal ideals of $K[X_1, \dots, X_n]$ are the ideals of the form $(X_1 - a_1, \dots, X_n - a_n)$.
3. (Weak Nullstellensatz) If I is a proper ideal of $K[X_1, \dots, X_n]$, then $V(I)$ is not empty.
4. (Strong Nullstellensatz) If I is an ideal of $K[X_1, \dots, X_n]$ then $IV(I) = \sqrt{I}$.
(2)⇒(3): For I a proper ideal, let J be a maximal ideal containing it. Then $V(J) \subseteq V(I)$ so $J = (X_1 - a_1, \dots, X_n - a_n)$, $a \in V(J)$.
</td>
</tr>
</table>

(3)⇒(4): Rabinowitsch Trick:

1. Let $f \in IV(I)$. Let $f_1, \dots, f_m$ be a generating set for $K[X_1, \dots, X_n, Y]$. Let I^* be the ideal generated by $f_1, \dots, f_m, 1 - Yf$.
2. $V(I^*) = \phi$
    a. If $(a_1, \dots, a_n, a_{n+1}) \in A^{n+1}$ and $(a_1, \dots, a_n) \in V(I)$, then $(a_1, \dots, a_n, a_{n+1}) \notin V(I^*)$ since it is not a zero of $1 - Yf$.
    b. If $(a_1, \dots, a_n) \notin V(I)$ then $(a_1, \dots, a_n, a_{n+1}) \notin V(I^*)$ (an even weaker statement).
3. Using the weak Nullstellensatz (see below), we can write
$$1 = \sum_{i=1}^{m} g_i f_i + h(1 - Yf)$$
since $V(I^*) = \phi \Rightarrow 1 \in I^* = K[X_1, \dots, X_n, Y]$.
4. Set $Y = 1/f$, and multiply to clear denominators
$$f^r = \sum_{i=1}^{m} h_i(X_1, \dots, X_n) f_i(X_1, \dots X_n) \in I$$

(4)⇒(3): The radical of an ideal is the intersection of all prime ideals containing I. I is in a maximal, prime ideal P; so is $\sqrt{I}$, so $\sqrt{I}$ is proper. $IV(I)$ is proper by (4), so $V(I) \neq \phi$.

(3)⇒(2): For I maximal, there is $a \in V(I)$. Since I is maximal, it must be in $(X_1 - a_1, \dots, x_n - a_n)$.

(1)⇒(2): Let I be a maximal ideal. K can be imbedded via $c \rightsquigarrow c + I$ in $K[X_1, \dots, X_n]/I$; by the corollary to Noether Normalization Lemma, this is a finite extension of K so must be K (since it is algebraically closed). Then $X_i + I = a_i + I \Rightarrow X_i - a_i \in I$, $(X_1 - a_1, \dots, X_n - a_n) \subseteq I$, with equality since the LHS is maximal.

(2)⇒(1): If f is a nonconstant polynomial in $K[X_1]$ with no root in K, regard it as a polynomial in $K[X_1, \dots, X_n]$ with no root in A^n. Then I is in a maximal ideal $(X_1 - a_1, \dots, X_n - a_n)$, so has root $X_1 = a_1$.

<u>Combinatorial Nullstellensatz:</u> Let F be a field, $f \in F[X_1, \dots, X_n]$ and let $S_1, \dots, S_n$ be nonempty subsets of F.

1. If $f(s_1, \dots, s_n) = 0$ for all $(s_1, \dots, s_n) \in S_1 \times \cdots \times S_n$ (i.e. $f \in V(S_1 \times \cdots \times S_n)$) then f lies in the ideal generated by the polynomials $g_i(X_i) = \prod_{s \in S_i}(X_i - s)$. The polynomials $h_1, \dots, h_n$ satisfying
$$f = g_1 h_1 + \cdots + g_n h_n$$
can be chosen so that $\deg(h_i) \leq \deg(f) - \deg(g_i)$ for all i. If $g_1, \dots, g_n \in R[X_1, \dots, X_n]$ for some subring $R \subseteq F$, we can choose $h_i \in R[X_1, \dots, X_n]$.
    a. The $s \in S_i$ are all zeros of g_i of degree $|S_i|$ so by subtracting multiples of g_i every X_i^k in f can be replaced with a linear combination of $1, \dots, x_i^{|S_i|-1}$. Then by counting zeros the result is actually 0; i.e. f is in the form above.
2. If $\deg(f) = t_1 + \cdots + t_n$ where t_i are nonnegative integers with $t_i < |S_i|$, and if the coefficient of $X_1^{t_1} \cdots X_n^{t_n}$ is not 0, then there exist $s_i \in S_i$ so that $f(s_1, \dots, s_n) \neq 0$, i.e. $f \notin f \in V(S_1 \times \cdots \times S_n)$.

4 Fields

Examples of Fields

An **extension** K of a field F (also denoted K/F) is a field containing F.

- Number field: subfield of $\mathbb{C}$
- Finite field: finitely many elements
- Function field: Extensions of $\mathbb{C}(t)$ of rational functions

4-1 Fundamental Theorem of Algebra

Fundamental Theorem of Algebra: Every nonconstant polynomial with complex coefficients has a complex zero. Thus, the field of complex numbers is algebraically closed, and every polynomial in $\mathbb{C}[x]$ splits completely.

Pf. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Let $x = re^{\theta i}$- the parameterization of a circle about the origin. $|f(x) - x^n|$ is small for large r, so for large r, $f(x)$ winds around the origin n times as θ goes from 0 to $2\pi n$.[2] (f is a person walking a dog on a circular path n times around the origin. The dog will also walk around the origin n times provided the leash is shorter than the radius.) For small r, $f(x)$ makes a small loop around a_0, and winds around the origin 0 times. For some intermediate value, $f(x)$ will pass through the origin.

4-2 Algebraic Elements

Let K be an extension, and α be an element of K. α is **algebraic** over F if it is the zero of a polynomial in $F[x]$, and **transcendental** otherwise. α is transcendental iff the substitution homomorphism $\varphi: F[x] \to K$ is injective.

$F(\alpha)$ is the smallest subfield of K that contains F and α. The irreducible polynomial f of α over F is the monic polynomial of lowest degree in $F[x]$ having α as a zero.

- Any polynomial in $F[x]$ having α as a zero divides f.
- $F[x]/(f)$ is an extension field of F with x a root of $f(x) = 0$. The substitution map $F[x]/(f) \to F[\alpha]$ is an isomorphism, so $F[x]/(f) \cong F(\alpha)$. [*]
- For every polynomial in F[x], there is an extension field in which it splits (factors) completely, i.e. every polynomial has a splitting field.
- If f has degree n then $F(\alpha)$ is a vector space with dimension n and basis $(1, \alpha, \dots, \alpha^{n-1})$.
- Let α, β be elements of $K/F, L/F$ algebraic over F. There is an isomorphism of fields $F(\alpha) \to F(\beta)$ sending $\alpha \rightsquigarrow \beta$ iff α, β have the same irreducible polynomial.

Let K, L be extensions of F. A **F-isomorphism** is an isomorphism $\varphi: K \to L$ that restricts to the identity on F. Then K and L are isomorphic as field extensions.

If α is a zero of f in K, then $\varphi(\alpha)$ is a zero of f.

4-3 Degree of a Field Extension

The **degree** $[K:F]$ is the dimension of K as an F-vector space.

- If α is algebraic over F, then $[F(\alpha):F]$ is the degree of the irreducible polynomial of α over F, and if α is transcendental, $[F(\alpha):F] = \infty$.
- $[K:F] = 1$ iff $F = K$.

---

[2] i.e. it is homotopic to the loop going around the origin n times in $\mathbb{C} - \{0\}$.

- If $[K:F] = 2$ then K can be obtained by adjoining a square root δ of an element in F: $\delta^2 \in F$
- <u>Multiplicative property:</u> If $F \subseteq K \subseteq L$, then $[L:F] = [L:K][K:F]$.
    - If K is a finite extension of F, and $\alpha \in K$, then the degree of α divides $[K:F]$.
    - If $\alpha \in L$ is algebraic over F, it is algebraic over K with degree less than or equal to its degree over F.
    - A field extension generated by finitely many algebraic elements is a finite extension.
    - The set of elements of K that are algebraic over F is a subfield of K.
- Let L be an extension field of F, and let K, F' be subfields of L that are finite extensions of F. Let $[K':F] = N, [K:F] = m, [F':F] = n$. Then m and n divide N, and $N \le mn$.

$$\begin{tikzcd}
 & K' \arrow[dl, dash, "\le n"'] \arrow[dr, dash, "\le m"] \arrow[dd, dash, "N \le mn"] & \\
K \arrow[dr, dash, "m"'] & & F' \arrow[dl, dash, "n"] \\
 & F &
\end{tikzcd}$$

Finding the Irreducible Polynomial of γ
(The dum way) Compute powers of γ, and find a relation between them.
(The smart way)

1. If $\gamma = a_1 + \cdots + a_n, a_1 \cdots a_n$ where each a_1 is algebraic (for example a *n*th root), then its conjugates (other zeros of the irreducible polynomial) are in the form $b_1 + \cdots + b_n, b_1 \cdots b_n$, respectively where b_i is a conjugate of a_i. (Not all these may be conjugates.)
2. The irreducible polynomial is $\prod_{\gamma' \text{ conjugate of } \gamma}(x - \gamma')$. [Note: This gives an elementary proof of the fact that the algebraic numbers/ integers form a field/ ring. For a, b algebraic, expand the product $(x - a' - b')$, a', b' running over the conjugates of a, b, and use the Fundamental Theorem on Symmetric Polynomials.]

4-4

Application: Constructions!

Rules:

1. Two points (0,0) and (1,0) are given (constructed).
2. If P, Q have been constructed, we can draw (construct)
    a. the line through them
    b. a circle with center at P and passing through Q.
3. Points of intersection of constructed lines and circles are constructed.
4. A number is constructible if (a,0) is constructible.

Finding all constructible numbers:

1. If $P = (a_0, a_1), Q = (b_0, b_1)$ have coordinates in F, then the line in (2a) is defined by a linear equation with coefficients in F, while the circle in (2b) is defined by a quadratic equation with coefficients in F.
2. The point of intersection of two lines/ circles whose equations have coefficients in F has coordinates in a real quadratic extension of F.
3. Let P be a constructible point. There is a chain of fields $\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_n = K$ such that
    a. K is a subfield of $\mathbb{R}$.
    b. The coordinates of P are in F_n.
    c. $[F_{i+1}:F_i] = 2$, and $[K:\mathbb{Q}] = 2^n$.

Thus a constructible number has degree over $\mathbb{Q}$ a power of 2.

4. Conversely, if a chain of fields satisfies the conditions above, then every element of K is constructible.

Examples:

1. Trisecting the angle with compass and straightedge is impossible. $\cos 20°$ is not constructible.
2. For p prime, a regular p-gon can be constructed iff $p = 2^r + 1$.

4-5 Finite Fields

A finite field is a vector space over $\mathbb{F}_p$ for some prime p, so has order $q = p^r$. The (unique) field of order q is denoted by $\mathbb{F}_q$.

1. The elements in a field of order q are roots of $x^q - x = 0$ (everything is modulo p).
    a. The multiplicative group $\mathbb{F}_q^\times$ of nonzero elements has order $q - 1$. The order of any element divides $q - 1$ so $\alpha^{q-1} = 0$ for any $\alpha \in \mathbb{F}_q$.
2. $\mathbb{F}_q^\times$ is a cyclic group of order $q - 1$.
    a. By the Structure Theorem for Abelian Groups, $\mathbb{F}_q^\times$ is a direct product of cyclic subgroups of orders $d_1 | \cdots | d_k$, and the group has exponent d_k. $x^{d_k} - 1 = 0$ has at most d_k roots, so $k = 1, d_k = q - 1$.
3. There exists a unique field of order q (up to isomorphism).
    a. Existence: Take a field extension where $x^q - x$ splits completely. If α, β are roots of $x^q - x = 0$ then $(\alpha + \beta)^q = \alpha + \beta$. Since -1 is a root, $-\alpha$ is a root. The roots form a field.
    b. Uniqueness: Suppose K, K' have order q. Let α be a generator of $K^\times$; $K = F(\alpha)$. The irreducible polynomial $f \in K[x]$ with root α divides $x^q - x$. $x^q - x$ splits completely in both K, K', so f has a root $\alpha' \in K'$. Then $F(\alpha) \cong F[x]/(f) \cong F(\alpha') = K'$.
4. A field of order p^r contains a subfield of order p^k iff $k|r$. (Note this is a relation between the exponents, not the orders.)
    a. $\mathbb{F}_{p^k} \subseteq \mathbb{F}_{p^r} \Rightarrow k|r$: Multiplicative property of the degree.
    b. $\mathbb{F}_{p^k} \subseteq \mathbb{F}_{p^r} \Leftarrow k|r$: $p^r - 1 | p^k - 1$. Cyclic $\mathbb{F}_{p^r}^\times$ contains a cyclic group of order p^k. Including 0, they are the roots of $x^{p^k} - x = 0$ and thus form a field by 3a.
5. The irreducible factors of $x^q - x$ over $\mathbb{F}_p$ are the irreducible polynomials g in $F[x]$ whose degrees divide r.
    a. $\Rightarrow$: Multiplicative property
    b. $\Leftarrow$: Let β be a root of g. If $k|r$, by (4), $\mathbb{F}_q$ contains a subfield isomorphic to $F(\beta)$. g has a root in $\mathbb{F}_q$ so divides $x^q - x$.
6. For every r there is an irreducible polynomial of degree r over $\mathbb{F}_p$.
    a. $\mathbb{F}_q (q = p^r)$ has degree r over $\mathbb{F}_p$, and has a cyclic multiplicative group generated by an element α. $\mathbb{F}_p(\alpha)$ has degree r over $\mathbb{F}_p$.

To compute in $\mathbb{F}_q$, take a root β of the irreducible factor of $x^q - x$ of degree r; $(1, \beta, \dots, \beta^{r-1})$ is a basis.

Let $W_p(d)$ be the number of irreducible monic polynomials of degree d in $\mathbb{F}_p$. Then by (2),

$$p^n = \sum_{d|n} d W_p(d).$$

By Möbius inversion,

	$$W_p(n) = \frac{1}{n}\sum_{d\mid n} \mu\left(\frac{n}{d}\right) p^d.$$ Primitive elements Let K be a field extension of F. An element $\alpha \in K$ such that $K = F(\alpha)$ is a **primitive element** for the extension. Primitive Element Theorem: Every finite extension of a field F contains a primitive element. Proof when F has characteristic 0: Show that if $K = F(\alpha, \beta)$ with $\alpha, \beta \in K$ then $\gamma = \beta + c\alpha$ is a primitive element for K over F. Let f, g be the irreducible polynomials of α, β, and α_i, b_j be the conjugates of α, β. For all but finitely many c, the numbers $\beta_j + c\alpha_i$ are all distinct. For such a value of c, to show that $\gamma = \beta + c\alpha$ is a primitive element, consider $h(x) = g(\gamma - cx) \in F(\gamma)$. $\gcd(f, h) = x - \alpha$ by choice of c, so $\alpha \in F(\gamma)$ as desired.

5 Modules

More structure→	No division	Division
More complex ↓	Ring	Field
	Module	Vector Space
	Algebra	Division Algebra

5-1 Modules

A left/right R-**module** ${}_RM/M_R$ over the ring R is an abelian group (M,+) with addition and scalar multiplication ($R \times M \to M$ or $M \times R \to M$) defined so that for all $r, s \in R$ and $x, y \in M$,

	Left	Right
1. Distributive	$r(x+y) = rx + ry$	$(x+y)r = xr + yr$
2. Distributive	$(r+s)x = rx + sx$	$x(r+s) = xr + xs$
3. Associative	$r(sx) = (rs)x$	$(xr)s = x(rs)$
4. Identity	$1x = x$	$x1 = x$

A (S,R)-**bimodule** ${}_SM_R$ has both the structure of a left S-module and right R-modules.
Modules are generalizations of vector spaces. All results for vector spaces hold except ones depending on division (existence of inverse in R). $S \subseteq M$ is linearly dependent if there exist $v_1, \ldots, v_n \in S$ such that $r_i v_i \neq 0$ and

$$r_1 v_1 + \cdots + r_n v_n = 0.$$

Again, a basis is a linearly independent set that generates the module. Note that if elements are linearly independent, it is not necessary that one element is a linear combination of the others, and bases do not always exist. Every basis for V (if it exists) contains the same number of elements. V is finitely generated if it contains a finite subset spanning V. The **rank** is the size of the smallest generating set.

A **submodule** of a R-module is a nonempty subset closed under addition and scalar multiplication. Viewing R as an R-module, the submodules of R are the ideals in R. In $\mathbb{Z}^n$, submodules correspond to lattices, with the area/volume of a fundamental parallelogram/parallelepiped equal to the determinant.

A **free module** with n generators has a basis with n elements. It is isomorphic to R^n.
An isomorphism preserves addition and scalar multiplication. Unlike vector spaces, not all finitely generated modules are isomorphic to some R^n.

Basic Theorems:

1. If W is a submodule of V, the quotient module V/W is a R-module, and the canonical map $\pi: V \to V/W$ is a homomorphism.
2. Mapping Property: Let $f: V \to V'$ be a homomorphism of R-modules with kernel containing W. There is a unique homomorphism $\bar{f}$ with $f = \bar{f} \circ \pi$.

$$\begin{tikzcd} V' \arrow[dr, dashed, "\bar{f}"] & \\ V \arrow[u, "\pi"] \arrow[r, "f"'] & G \end{tikzcd}$$

3. First Isomorphism Theorem: If f is surjective with kernel W, $\bar{f}$ is an isomorphism.
4. Correspondence Theorem: Let $f: V \to V'$ be a surjective homomorphism. There is a bijective correspondence between submodules of V' and submodules of V that containing $\ker f = W$: S with $W \subseteq S \subseteq V$ is associated with $f(S)$; $V/S \cong V'/f(S)$.

5. Second Isomorphism Theorem: Let S and T be submodules of M, and let $S+T = \{x+y : x \in S, y \in T\}$. Then $S+T$ and $S \cap T$ are submodules of M and
$$\frac{S+T}{T} \cong \frac{S}{S \cap T}$$
6. Third Isomorphism Theorem: Let $N \subseteq L \subseteq M$ be modules. Then $M/L \cong (M/N)/(L/N)$.

5-2

Structure Theorem

Matrices, invertible matrices, the general linear group, the determinant, and change of bases matrices all generalize to a ring R. However, a R-matrix A is invertible iff its determinant is a *unit*.

Properties of matrices in a field such as $\det(AB) = \det(A)\det(B)$ continue to hold in a ring, because they are polynomial identities.

Smith Normal Form

For a matrix over an Euclidean domain R [*] (such as $\mathbb{Z}$ or $F[t]$), elementary row/ column operations correspond to left and right multiplication by elementary matrices and include:

(1) Interchanging 2 rows/ columns
(2) Multiplying any row/ column by a unit
(3) Adding any multiple of a row/ column to another row/ column

However, note arbitrary division in R is illegal.

A $m \times n$ matrix is in **Smith** (or **Hermite**) **normal form** if

1. It is diagonal.
2. The entries $d_1, \ldots, d_n$ on the main diagonal satisfy $d_k | d_{k+1}, 1 \le k < \min(m,n)$. (Ones at the end may be 0.)

Every matrix is equivalent to a unique matrix N in normal form. For a $m \times n$ matrix A, follow this algorithm to find it:

1. Make the first column $\begin{bmatrix} p \\ 0 \\ \vdots \\ 0 \end{bmatrix}$.
   a. Choose the nonzero entry f in the first column that has the least norm.
   b. For each other nonzero entry p, use division to write $p = fq + r$, where r is the remainder upon division. Subtract q times the row with f from the row with p.
   c. Repeat a and b until there is (at most) one nonzero entry. Switch the first row with that row if necessary.
2. Put the first row in the form $[p \quad 0 \quad \cdots \quad 0]$ by following the steps above but exchanging the words “rows” and “columns”.
3. Repeat 1 and 2 until the first entry g is the only nonzero entry in its row and column. (This process terminates because the least degree decreases at each step.)
4. If g does not divide every entry of A, find the first column with an entry not divisible by g and add it to column 1, and repeat 1-4; the degree of “g” will decrease. Else, go to the next step.
5. Repeat with the $(m-1) \times (n-1)$ matrix obtained by removing the first row and column.

Solving $AX = B$ in R:

1. Write $A = QA'P^{-1}$, where A' is in normal form. Suppose the nonzero diagonal entries are $d_1, d_2, \ldots, d_k$.
2. The solutions X' of the homogeneous system $A'X' = 0$ are the vectors whose first k coordinates are 0.

3. The solutions of $AX = 0$ are in the form $X_h = PX'$.
4. The equation has a solution iff B is in the form $QY', Y' = \begin{bmatrix} r_1 d_1 \\ \vdots \\ r_k d_k \\ 0 \\ \vdots \end{bmatrix}$. Use linear algebra to find a particular solution X_p. (The condition guarantees that the entries are in R.) Then the solutions are $X_h + X_p$, for X_h a homogeneous solution.

Structure Theorem:
(a.k.a. Fundamental Decomposition Theorem)
Let M be a finitely generated module over the PID R (such as $\mathbb{Z}$ or $F[t]$). Then M is a direct sum of cyclic modules and a free module $C_1 \oplus \cdots \oplus C_k \oplus L$, where $C_i \cong R/(d_i)$. The cyclic modules can be chosen to satisfy either of the following conditions:
1. $d_1 | d_2 \cdots | d_k$
2. Each d_i is the power of an irreducible element.

5-3 Noetherian and Artinian Rings

The following conditions on a R-module V are equivalent:
1. Every submodule is finitely generated.
2. Ascending chain condition: There is no infinite strictly increasing chain $W_1 \subset W_2 \subset \cdots$ of submodules. (Pf. of ⇒: Union of chain finitely generated.)

A ring is **Noetherian** if every ideal of R is finitely generated. In a Noetherian ring, every proper ideal is contained in a maximal ideal.
Let φ be a homomorphism of R-modules.
1. If V is finitely generated and φ is surjective, then V' is finitely generated.
2. If $\ker \varphi, \operatorname{im} \varphi$ are finitely generated, so is V. (Pf. Take a generating set for the kernel and some preimage of a generating set for the image.)
3. In particular, if V is finitely generated, so is V/W. If V/W and W are finitely generated, so is V.

If R is Noetherian, then every submodule of a finitely generated R-module is finitely generated.
Pf. Using a surjective map $\varphi: R^m \to V$, it suffices to prove it for R^m. Induct on m. For the projection $\pi: R^m \to R^{m-1}$, the image and kernel are finitely generated.

A ring is **Artinian** if it satisfies the descending chain condition on ideals: There is no infinite strictly decreasing chain $I_1 \supset I_2 \supset \cdots$ of ideals.

5-4 Application 1: Abelian Groups

An abelian group corresponds to a $\mathbb{Z}$-module with integer multiplication defined by $nv = \underbrace{v + v + \cdots + v}_{n \text{ times}}$. Abelian groups and $\mathbb{Z}$-modules are equivalent concepts, so generalizing linear algebra for modules helps us study abelian groups.

If W is a free abelian group of rank m, and U is a subgroup, then U is a free abelian group of rank at most m.
Pf. Choose a (finite) set of generators $\beta = (u_1, \dots, u_n)$ for U and a basis $\gamma = (w_1, \dots, w_m)$ for W. Write $u_j = \sum_i w_i a_{ij}$. Then left multiplication by A is an surjective homomorphism $\mathbb{Z}^n \to \mathbb{Z}^m$. Diagonalizing A, we can find an explicit basis for U with at most $n \le m$ elements.

$$\begin{tikzcd} \mathbb{Z}^n \arrow[r, "A"] \arrow[d, dashed, "B"'] & \mathbb{Z}^m \arrow[d, "C"] \\ U \arrow[r, "i"] & W \end{tikzcd}$$

Generators and Relations

Let A be a matrix, and let AR^n denote the image of R^n under left multiplication by A. The module $V = R^m/AR^n$ is **presented** by the matrix A.

An abelian group G with n generators $v_1, \dots, v_n$ can be identified with a quotient module of $\mathbb{Z}^n$. The set of $[a_1, \dots, a_n]^T \in \mathbb{Z}^n$ such that

$$\sum_{i=1}^{n} a_i v_i = 0$$

forms a submodule of $\mathbb{Z}^n$. They are the relations in G, and form the kernel of the map $\mathbb{Z}^n \to G$. If $[a_{i1}, \dots, a_{in}]^T \in \mathbb{Z}^n$ generate this submodule, letting A be the matrix with these rows,

$$\sum_{i=1}^{n} b_i v_i = 0 \Leftrightarrow \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} = Av \text{ for some } v \in \mathbb{Z}^n$$

Then G corresponds to the module $\mathbb{Z}^n/A\mathbb{Z}^n$; G is **presented** by A. An abelian group that is presented by a matrix needs only satisfy the relations implied (through linearity) by the relations given by the columns of A. To determine a group from its presentation:

1. Use elementary row and column operations to write A in normal form.
2. Delete any columns of 0's (trivial relations).
3. If 1 is the only nonzero entry in its column, delete that row and column. (This is a relation of the form $v = 0$.)
4. If the diagonal entries are $d_1, \dots, d_k$, and there are l zero rows, then the group is isomorphic to $\mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_k} \oplus \mathbb{Z}^l \cong C_{d_1} \oplus \cdots \oplus C_{d_k} \oplus lC_\infty$.

Structure Theorem for Finitely Generated Abelian Groups:

a.k.a Unicity Theorem for Abelian Group Decomposition, Basis Theorem

A finitely generated abelian group V is the direct sum of cyclic subgroups and a free abelian group: $V = C_{d_1} \oplus \cdots \oplus C_{d_k} \oplus L$. The orders can be chosen uniquely to satisfy either of the following two conditions:

1. $1 < d_1 | d_2 \cdots | d_k$
2. All the d_i are prime power orders. (Uniqueness follows from counting orders in p-groups.)

5-5 Application 2: Linear Operators

A linear operator T on a F-vector space corresponds to a $F[t]$***-module with multiplication by a polynomial defined by*** $tv = T(v), f(t)v = [f(T)](v)$. A submodule corresponds to a T-invariant subspace. The structure theorem gives:

Rational Canonical Form:

Every linear operator T on finite-dimensional V has a **rational canonical form**.

$$[T]_\beta = \begin{bmatrix} C_1 & O & \cdots & O \\ O & C_2 & \cdots & O \\ \vdots & \vdots & & \vdots \\ O & O & \cdots & C_r \end{bmatrix}$$

where each C_i is the companion matrix of an invariant factor p_i. The rational canonical form

is unique under the condition $p_{i+1}|p_i$ for each $1 \le i < r$.
The **companion matrix** of the monic polynomial $p(t) = a_0 + a_1 t + \cdots + a_{k-1}t^{k-1} + t^k$ is $C(p) = \begin{bmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{k-1} \end{bmatrix}$ because the characteristic polynomial of C(p) is $(-1)^k p(t)$.
The product of the invariant factors is the characteristic polynomial of T.

5-6 Polynomial Rings in Several Variables

Let $R = \mathbb{C}[x_1, \ldots, x_k] = \mathbb{C}[X]$ ($X \in \mathbb{C}^k$), and V be a finitely generated R-module with presentation matrix $A(X)$. V is a free module of rank r iff $A(c)$ has rank $m - r$ at every point $c \in \mathbb{C}^k$.
The subspace $W(c)$ spanned by the columns varies continuously as c if the dimension does not “jump around.” Continuous families of vector spaces are **vector bundles**. V is free iff $W(c)$ forms a vector bundle over $\mathbb{C}^n$.

5-7 Tensor Products

Commutative Rings:
The **tensor product** $M \otimes_R N$ of R-modules M and N is the (unique) R-module T (along with a bilinear map $h: M \times N \to T$) satisfying the Universal Mapping Property: for any *bilinear map* $f: M \times N \to P$, there is a unique R-homomorphism $g: T \to P$ such that $f = gh$.

$$\begin{tikzcd} & T \arrow[d, "g"] \\ M \times N \arrow[ur, "h"] \arrow[r, "f"'] & P \end{tikzcd}$$

One way to construct it is as follows: Let F be the free module with basis $M \times N$, and let G be the submodule generated by $(x + x', y) - (x, y) - (x', y)$, $(x, y + y') - (x, y) - (x, y')$, $(rx, y) - r(x, y)$, $(x, ry) - r(x, y)$ for all $x, x' \in M; y, y' \in N, r \in R$. Then $M \otimes_R N = F/G$; $x \otimes y$ denotes $(x, y) + G$. The relations make $x \otimes y$ linear:

1. $(x + x') \otimes y = x \otimes y + x' \otimes y$
2. $x \otimes (y + y') = x \otimes y + x \otimes y'$
3. $r(x \otimes y) = rx \otimes y = x \otimes ry$

Note that in general, an element of $M \otimes N$ is a sum (linear combination) of elements in the form $x \otimes y$.

Basic properties (prove using UMP)

1. $M \otimes N \cong N \otimes M$
2. $(M \otimes N) \otimes P \cong M \otimes (N \otimes P)$
3. $M \otimes (N \oplus P) \cong (M \otimes N) \oplus (M \otimes P)$
4. $R \otimes_R M \cong M, R^m \otimes M \cong M^m$ where A^m means the direct sum of m copies of A.
5. $R^m \otimes R^n = R^{mn}$.

The tensor product $f_1 \otimes f_2$ of homomorphisms $f_1: M_1 \to N_1, f_2: M_2 \to N_2$ is the map $f: M_1 \otimes M_2 \to N_1 \otimes N_2$ such that $f(x_1 \otimes x_2) = f_1(x_1) \otimes f_2(x_2)$. Note that $(g_1 \otimes g_2) \circ (f_1 \otimes f_2) = (g_1 \circ f_1) \otimes (g_2 \circ f_2)$. When applied to the linear transformations corresponding to the homomorphisms, the tensor (Kronecker) product of $p \times q$ matrix A and $r \times s$ matrix B is

$A \otimes B = \begin{bmatrix} a_{11}B & \cdots & a_{1q}B \\ \vdots & \ddots & \vdots \\ a_{p1}B & \cdots & a_{pq}B \end{bmatrix}$. The ordering of the basis is $v_1 \otimes w_1, \ldots, v_1 \otimes w_q, \ldots, v_p \otimes w_q$.

For the tensor product of algebras, multiplication is given by $(a \otimes b)(a' \otimes b') = aa' \otimes bb'$.

Noncommutative rings:
The **tensor product** $M \otimes_R N$ of *right* R-module M_R and *left* R-module ${}_RN$ is an abelian group T (along with a bilinear map $h: M \times N \to T$) satisfying the Universal Mapping Property: for any *biadditive, R-balanced map* $f: M \times N \to P$

1. $f(x + x', y) = f(x, y) + f(x', y), f(x, y + y') = f(x, y) + f(x, y')$
2. $f(xr, y) = f(x, ry)$

there is a unique abelian group homomorphism $g: T \to P$ such that $f = gh$.

$$\begin{tikzcd} & T \arrow[d, "g"] \\ M \times N \arrow[ur, "h"] \arrow[r, "f"'] & P \end{tikzcd}$$

One way to construct it is as follows: Let F be the free module with basis $M \times N$, and let G be the submodule generated by $(x + x', y) - (x, y) - (x', y)$, $(x, y + y') - (x, y) - (x, y')$, $(xr, y) - (x, ry)$ for all $x, x' \in M; y, y' \in N, r \in R$. Then $M \otimes_R N = F/G$; $x \otimes y$ denotes $(x, y) + G$. The relations make $x \otimes y$ biadditive and R-balanced:

1. $(x + x') \otimes y = x \otimes y + x' \otimes y$
2. $x \otimes (y + y') = x \otimes y + x \otimes y'$
3. $xr \otimes y = x \otimes ry$

If M is a (S,R) bimodule and N is a (R,T) module, then $M \otimes N$ is a S-T bimodule. Definitions generalize to more modules with multiadditive balanced maps.
The above properties all hold except for commutativity; (2) is replaced by $M \otimes_R N \otimes_S P \cong (M \otimes_R N) \otimes_S P \cong M \otimes_R (N \otimes_S P)$.

6	Galois Theory

6-1 Symmetric Polynomials

Symmetric Polynomials
A **symmetric** polynomial is fixed by every permutation of the variables.
The **elementary symmetric polynomial** in n variables $x_1, \dots, x_n$ of degree k is

$$s_k = \sum_{1 \le i(1) < \cdots < i(k) \le n} x_{i(1)} \cdots x_{i(k)}.$$

Vieta's Theorem: If

$$(x-\alpha_1)\cdots(x-\alpha_n) = x^n + a_1 x^{n-1} + \cdots + a_n$$

Then $\alpha_i = (-1)^i a_i$.

Newton's identities: Let $w_k = \alpha_1^k + \cdots + \alpha_n^k$. Then

$$w_k - s_1 w_{k-1} + \cdots + (-1)^k s_k w_1 + (-1)^k k s_k = 0$$

Fundamental Theorem of Symmetric Polynomials: Every symmetric polynomial in $R[x]$ can be written in a unique way as a polynomial in the elementary symmetric polynomials. The polynomial will be in $R[x]$.
Pf. Introduce a lexicographic ordering of the monomials and use induction.
Corollaries:

1. If $f(x) \in F[x]$ has roots $\alpha_1, \dots, \alpha_n$ in $K \supseteq F$, and $g(x_1, \dots, x_n) \in F[x_1, \dots, x_n]$ is a symmetric polynomial, then $g(\alpha_1, \dots, \alpha_n) \in F$.
2. If $p_1, \dots, p_k$ is the orbit of p_1 for the operation of the symmetric group on the variables, and $h(x_1, \dots, x_k)$ is a symmetric polynomial, then $h(p_1, \dots, p_k)$ is a symmetric polynomial.

6-2 Discriminant

If $P(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ has roots $\alpha_1, \dots, \alpha_n$, then the **discriminant** of P is

$$D = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2.$$

Since D is a symmetric polynomial in the u_i, it can be written in terms of the elementary symmetric polynomials. (It can always be defined in terms of Δ whether or not P splits completely.)

$$D(\alpha_1, \dots, \alpha_n) = \Delta(s_1, \dots, s_n) = \Delta(-a_1, \dots, (-1)^n a_n)$$

Ex.

1. $D(x^2 + bx + c) = b^2 - 4c$.
2. $D(x^3 + px + q) = -4p^3 - 27q^2$.

6-3 Galois Group

Assume fields have characteristic 0.
The F-automorphisms of an extension K form the **Galois group** $G(K/F)$ of K over F. K/F is a **Galois extension**[3] if $|G(K/F)| = [K:F]$.
Ex. $G(\mathbb{C}/\mathbb{R}) = \{I, \text{conjugation}\}$.
Any two splitting fields of f over F are isomorphic.

[3] In general (when K is not necessarily a finite extension) a Galois extension is defined as a normal, separable field extension. A **separable** polynomial has no repeated roots in a splitting field; n element is separable over F if its minimal polynomial is separable; a separable field extension has every element separable over F.

	Pf. (a) An extension field contains at most one splitting field of f over F. (b) Suppose K_1, K_2 are 2 splitting fields. Take a primitive element $\gamma \in K_1$ with irreducible polynomial g. Choose an extension L of K_2 so that g has a root γ'. Then use (a).
6-4	Fixed Fields Let H be a group of automorphisms of a field K. The **fixed field** of H, K^H, is the set of elements of K fixed by every group element. $$K^H = \{\alpha \in K \mid \sigma(\alpha) = \alpha\ \forall \sigma \in H\}$$ <u>Fixed Field Theorem:</u> 1. $[K: K^H] = \|H\|$: The degree of K over K^H is equal to the order of the group. 2. $H = G(K/K^H)$: K is a Galois extension of K^H with Galois group H. Pf. 1. Let $\beta_1 \in K$ with H-orbit $\beta_1, \dots, \beta_r$. For any i, there is $\sigma \in H$ with $\sigma(\beta_1) = \beta_i$. Thus $x - \beta_i \| h$. Since $g(x) = (x - \beta_1) \cdots (x - \beta_r) \in K^H[x]$ by symmetry, g is the irreducible polynomial for β_1 over K^H. r divides the order of H. 2. If $[K: F] = \infty$, there exist elements in K whose degrees over F are arbitrarily large. 3. By (1), K/K^H is algebraic, so by (2), $[K: K^H]$ is finite. The stabilizer of a primitive element is trivial, so the orbit has order $n = \|H\|$. By (1), γ has degree n over K^H. Then $[K: K^H] = n$. 4. Let $G = G(K/K^H)$. Then $H \subseteq G \Rightarrow K^G \subseteq K^H$. By definition, every element of G acts as the identity on K^H so $K^H \subseteq K^G$. <u>Lüroth's Theorem:</u> Let $F \supset \mathbb{C}$ be a subfield of the field $\mathbb{C}(t)$ of rational functions. Then F is a field $\mathbb{C}(u)$ of rational functions.
6-5	Galois Extensions and Splitting Fields Splitting Fields A **splitting field** of $f \in F[x]$ over F is an extension K/F such that 1. f splits completely in K: $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$, $\alpha_i \in K$. 2. $K = F(\alpha_1, \dots, a_n)$ A splitting field is a finite extension, and every finite extension is contained in a splitting field. <u>Splitting Theorem:</u> If K is the splitting field of some $f(x) \in F[x]$, then any irreducible polynomial $g(x) \in F[x]$ with one root in K splits completely in K. (A field satisfying the latter condition is called a **normal** extension of F.) Conversely, any finite normal extension is a splitting field. Pf. Suppose $g(x)$ has the root $\beta \in K$. Then $p_1(\alpha_1, \dots, \alpha_n) = \beta$ for some $p_1 \in F[x_1, \dots, x_n]$. Let $p_1, \dots, p_k$ be the orbit of p_1 under the symmetric group. Then $\prod_{i=1}^{k}\left(x - p_i(\alpha_1, \dots, \alpha_n)\right) \in F[x]$ by symmetry so it is divisible by $g(x)$, the irreducible polynomial of β. If K is an extension of F, then an intermediate field satisfies $F \subseteq L \subseteq K$. A proper intermediate field is neither F nor K. Note $F \subseteq L \Rightarrow G(K/L) \subseteq G(K/F)$. The order of $G = G(K/F)$ divides $[K: F]$, since $\|G\| = [K: K^G]$ and $[K: F] = [K: K^G][K^G: F]$. Characteristic Properties of Galois Extensions: For a finite extension K, the following are equivalent. 1. K/F is a Galois extension. 2. $K^G = F$ where $G = G(K/F)$.

3. K is a splitting field over F.

Pf. (1)⇔(2): By the Fixed Field Theorem, $|G| = [K:K^G]$.
(1)⇔(3): Let γ_1 be a primitive element for K, with irreducible polynomial f. Let $\gamma_1, \dots, \gamma_r$ be the roots of f in K. There is a unique F-automorphism σ_i sending $\gamma_1 \rightsquigarrow \gamma_i$ for each i, and these make up the group $G(K/F)$. Thus the order of $G(K/F)$ is equal to the number of conjugates of γ_1 in K. So K/F Galois⇔ $r = |G| = [K:K^G] \Leftrightarrow f$ (degree r) splits completely in K⇔ K is a splitting field.

If K/F is a Galois extension, and $g \in F[x]$ splits completely in K with roots $\beta_1, \dots, \beta_r$, then

- G operates on the set of roots $\{\beta_i\}$.
- G operates faithfully if K is a splitting field of g over F.
- G operates transitively if g is irreducible over F.
- If K is the splitting field of irreducible g, then G embeds as a transitive subgroup of S_r.

6-6 Fundamental Theorem

<u>Fundamental Theorem of Galois Theory:</u> Let K be a Galois extension of a field F, and let $G = G(K/F)$. Then there is a bijection between subgroups of G and intermediate fields, defined by

$$H \rightsquigarrow K^H$$
$$G(K/L) \leftsquigarrow L$$

Let $L = K^H$ (the fixed field of a subgroup H of G). L/F is a Galois extension iff H is a normal subgroup of G. If so, $G(L/F) \cong G/H$.

$G = G(K/F)$ operates on K fixing F. $\left\{ \begin{array}{l} \text{K} \\ \quad \} \; H = G(K/L) \text{ operates on K fixing L.} \\ \text{L} \\ \quad \} \; H \text{ normal: } G/H \cong G(L/F) \text{ operates here.} \\ \text{F} \end{array} \right.$

Pf. Let γ_1 be a primitive element for L/F and let g be the irreducible polynomial for γ_1 over F. Let the roots of g in K be $\gamma_1, \dots, \gamma_r$. For $\sigma \in G, \sigma(\gamma_1) = \gamma_i$, the stabilizer of γ_i is $\sigma H \sigma^{-1}$. Thus $\sigma H \sigma^{-1} = H \Leftrightarrow \gamma_i \in L = K^H$. H is normal⇔All $\gamma_i \in L \Leftrightarrow L/F$ Galois. Restricting σ to L gives a homomorphism $\varphi: G \to G(L/F)$ with kernel H.

6-7 Roots of Unity

Let $\zeta_n = e^{\frac{2\pi i}{n}}$. $F(\zeta_n)$ is a **cyclotomic field**. For p prime, the Galois group of $F(\zeta_p)$ is isomorphic to $\mathbb{F}_p^\times$, of order $p-1$.
Ex. For $p = 2^r + 1$, G is cyclic of order 2^r. Let ξ be a primitive root modulo p, and $\sigma(\zeta) = \zeta^\xi$. The degree of each extension in the following chain is 2: $F = K^{\langle\sigma\rangle} \subset K^{\langle\sigma^2\rangle} \subset \cdots \subset K^{\langle\sigma^{2^{r-1}}\rangle} \subset K^{\langle\sigma^{2^r}\rangle} = K$. $\cos\frac{2\pi}{p}$ generates $K^{\langle\sigma^{2^{r-1}}\rangle}$ so the regular p-gon can be constructed.

<u>Kronecker-Weber Theorem:</u> Every Galois extension of $\mathbb{Q}$ whose Galois group is abelian is contained in a cyclotomic field $\mathbb{Q}(\zeta_n)$.
Ex. If p is prime and L is the unique quadratic extension of $\mathbb{Q}$ in $\mathbb{Q}(\zeta_p)$,

1. If $p \equiv 1 \pmod 4$ then $L = \mathbb{Q}(\sqrt{p})$.
2. If $p \equiv 3 \pmod 4$ then $L = \mathbb{Q}(i\sqrt{p})$.

Show this by letting σ be a generator as before, take the orbit sums of the roots for $\langle\sigma^2\rangle$.

Kummer Extensions

Let F be a subfield of $\mathbb{C}$ containing $\zeta = e^{2\pi i/p}$, and let K/F be a Galois extension of degree p. Then K is obtained by adjoining a pth root (some β with $\beta^p \in F$).
Pf.

1. For $b \in F$, $g(x) = x^p - b$ is either irreducible in F, or splits completely in F. (Take $I \neq \sigma \in G(K/F)$; then $\sigma^k(\beta) = \zeta^{kv}\beta$ for some $v \neq 0$, so G operates transitively on the roots of g.)
2. K is a vector space over F; each $\sigma \in G$ is a linear operator. Choose a generator σ. $\sigma^p = I$ implies that the matrix is diagonalizable and all eigenvalues are powers of ζ. Let β be an eigenvector with eigenvalue $\lambda \neq 1$; then $\sigma(\beta^p) = \beta^p \Rightarrow \beta^p \in K^G = F$, but $\beta \notin F$, so $F(\beta) = K$.

6-8

Cubic Equations

Let K be the splitting field of an irreducible cubic polynomial f over F with roots $\alpha_1, \alpha_2, \alpha_3$, let D be the discriminant of f, and let $G = G(K/F)$.

If…	$[K:F]$	$G \cong$	Chain	Proper intermediate fields
D is not a square in F	3	$A_3 \cong C_3$	$F \subset F(\alpha_1) = K$	None
D is a square in F	6	$G \cong S_3$	$F \subset F(\alpha_1)$ $\subset F(\alpha_1, \alpha_2) = K$	$F(\alpha_1), F(\alpha_2), F(\alpha_3), F(\delta)$

Pf. Let $\delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3) = \pm\sqrt{D}$. $\delta \in F \Leftrightarrow \delta$ fixed by every element of G $\Leftrightarrow$ only even permutations in G.
In general, for an irreducible polynomial of any degree, $\delta = \sqrt{D} \in F \Leftrightarrow$ G contains only even permutations.

Cubic Formula
To solve $x^3 + a_2x^2 + a_1x + a_0 = 0$ first substitute $x = y - a_2/3$ (Tschirnhausen transformation) to put it in the form $x^3 + px + q = 0$.
For roots $\alpha_1, \dots, \alpha_n$, $z = \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3$, $z' = \alpha_1 + \omega^2\alpha_2 + \omega a_3$ are eigenvectors for $\sigma = (123)$. Let $A = \sum_{\text{cyc}} \alpha_1^3$, $B = \sum_{\text{cyc}} \alpha_1^2 \alpha_2$, $C = \sum_{\text{cyc}} \alpha_1\alpha_2^2$. Then $B - C = \sqrt{D}$. Express $A, B + C$ in terms of elementary symmetric polynomials, apply Vieta's formula, and solve for A, B, C. Find z^3, then take the cube root:

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} - \sqrt[3]{\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}$$

6-9

Quartic Equations

Let $f \in F[x]$ be an irreducible quartic polynomial.
Let $\beta_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4, \beta_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4, \beta_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3$.
$g(x) = (x - \beta_1)(x - \beta_2)(x - \beta_3)$ is the **resolvent cubic** of f.

What is $G = G(K/F)$?

	D square	D not square
g reducible	D_2 (g splits completely)	D_4 or C_4 (g has 1 root in F)
g irreducible	A_4	S_4

$D_2 = \{I, (12)(34), (13)(24), (14)(23)\}$
For the ambiguous case, let $\gamma = \alpha_1\alpha_2 - \alpha_3\alpha_4, \epsilon = \alpha_1 + \alpha_2 - \alpha_3 - \alpha_4$. $\delta\gamma$ or $\delta\epsilon$ is a square in F iff $G = C_4$.

Pf. The β_i are distinct since $\beta_1 - \beta_2 = (\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3)$. S_4 operates on $B = \{\beta_i\}$, giving $\varphi: S_4 \to S_3$. If g irreducible, G operates transitively on B, so $3||G|$.

Special case: $f(x) = x^4 + bx^2 + c = 0$. Then the roots are $\alpha_1, \alpha_2 = \sqrt{\frac{-b \pm \sqrt{b^2-4c}}{2}}$, $\alpha_3 = -\alpha_1$, and $\alpha_4 = -\alpha_2$, so $G \subseteq D_4$. Look at expressions such as $\alpha_1\alpha_2$.

Quartics are solvable in the following way:

1. Adjoin $\delta = \sqrt{D}$.
2. Use Cardano's formula to solve for a root of the resolvent cubic $g(x)$ and adjoin it.
3. The Galois group over the field extension K is a subgroup of D_2. At most 2 more square root extensions suffice.

6-10

Quintic Equations and the Impossibility Theorem

Quintic Equations

<u>Impossibility Theorem:</u> The general quintic equation is not solvable by radicals.

Pf.

1. The following are equivalent: (We say that α is solvable [by radicals] over F.)
    a. There is a chain of subfields $F = F_0 \subset F_1 \subset \cdots \subset F_r = K \subset \mathbb{C}$ such that $\alpha \in F_r, F_{j+1} = F_j(\beta_{j+1})$ where a power of β_{j+1} is in F_j.
    b. There is a chain of subfields $F = F_0 \subset F_1 \subset \cdots \subset F_r = K \subset \mathbb{C}$ such that $\alpha \in F_r$, and F_{j+1} is a Galois extension of F_j of prime degree. (Equivalent to (a) by Kummer's Theorem.)
    c. There is a chain of subfields $F = F_0 \subset F_1 \subset \cdots \subset F_r = K \subset \mathbb{C}$ such that $\alpha \in F_r$, and F_{j+1} is an abelian Galois extension of F_j.
2. Let $f, g \in F[x]$, and let F' be a splitting field of fg. K' contains a splitting field K of f, and a splitting field F' of g. Let $G = G(K/F), H = G(F'/F), \mathcal{G} = G(K'/F)$. Then G, H are quotients of $\mathcal{G}$ (Fundamental Theorem) and $\mathcal{G}$ is isomorphic to a subgroup of $G \times H$.

$$\begin{tikzcd} & K' \arrow[dl, dash] \arrow[dr, dash] \arrow[dd, dash, "\mathcal{G}"'] & \\ K \arrow[dr, dash, "G"'] & & F' \arrow[dl, dash, "H"] \\ & F & \end{tikzcd}$$

    a. Let the canonical maps $\mathcal{G} \to G, \mathcal{G} \to H$ send $\sigma \rightsquigarrow \sigma_f, \sigma \rightsquigarrow \sigma_g$. Then $\mathcal{G} \to G \times H$ defined by $\sigma \rightsquigarrow (\sigma_f, \sigma_g)$ is injective.
3. Let $f \in F[x]$ be a polynomial whose Galois group G is simple and nonabelian. Let F' be a Galois extension of F with Galois group of prime order, and let K' be a splitting field of f over F'. Then $G(K'/F') \cong G$. In other words, *we cannot make progress solving for the roots by replacing F by a prime extension.*
    a. From (3), $|G|$ divides $|\mathcal{G}|$ and $|\mathcal{G}|$ divides $|G \times H| = p|G|$. 2 cases:
        i. $|\mathcal{G}| = |G|$: Then $|K'| = |K|$, H is a quotient of $|\mathcal{G}|$, contradicting simplicity.
        ii. $|\mathcal{G}| = |G \times H|$: Then $G = G(K'/F')$.
4. If f is an irreducible quintic polynomial with Galois group A_5 or S_5 then the roots of f are not solvable over F.
    a. Adjoin $\delta = \sqrt{D}$ to reduce to A_5 case.
    b. A_5 is simple.
    c. By (3), in the "solvable series," each field extension has Galois group A_5. f remains irreducible after each extension.
5. There exists a polynomial with Galois group S_5.

	a. A subgroup of S_5 containing a 5-cycle and transposition is the whole group. b. If f is a quintic irreducible polynomial with exactly 3 real roots, then the Galois group is S_5 by (a). c. Example: $x^5 + 16x + 2$. In general, a polynomial equation over a field of characteristic 0 is solvable by radicals iff its Galois group is a solvable group. In (4) above, the Galois group after adjoining an element is a subgroup of the previous one, with factor group prime cyclic.
6-11	Transcendence Theory Lindemann–Weierstrass Theorem: If $\alpha_1, \ldots, \alpha_n$ are algebraic numbers linearly independent over the rational numbers $\mathbb{Q}$, then $e^{\alpha_1}, \ldots, e^{\alpha_n}$ are algebraically independent over $\mathbb{Q}$; in other words the extension field $\mathbb{Q}(e^{\alpha_1}, \ldots, e^{\alpha_n})$ has transcendence degree n over $\mathbb{Q}$. [Incomplete]

7 Algebras

An **algebra** $\mathcal{A}$ over a ring R is a module $\mathcal{A}$ over R with multiplication defined so that for all $x, y, z \in \mathcal{A}, c \in R$,

1. Associative	$x(yz) = (xy)z$
2. Distributive	$x(y+z) = xy + xz, (x+y)z = xz + yz$
3.	$c(xy) = (cx)y = x(cy)$

If there is an element $1 \in \mathcal{A}$ so that $1x = x1 = x$, then 1 is the identity element. $\mathcal{A}$ is commutative if $xy = yx$. $\mathcal{A}$ is a **division algebra** if each element has an inverse $(xx^{-1} = 1)$.

7-1 Division Algebras

<u>Frobenius Theorem:</u> The only finite-dimensional division algebras D over the real numbers are $\mathbb{R}$ (the real numbers), $\mathbb{C}$ (the complex numbers) and H (the quaternions).

<u>Pf.</u> Associate with each $d \in D$ the linear transformation $T_d(x) = dx$.

1. Lemma: The set V of all $a \in D$ such that $a^2 \in \mathbb{R}, a^2 \leq 0$ forms a subspace of codimension 1 (i.e. $\dim_{\mathbb{R}}(V/D) = 1$).
   Proof: Let p be the characteristic polynomial of T_a. By Cayley-Hamilton, $p(T_a) = 0$. Since there are no zero factors in D, one irreducible real factor of p must be 0 at a. If the factor is linear $(x - r)$, then $a \in \mathbb{R}, a = 0$. If the factor is irreducible quadratic $(x^2 - 2\Re(r)x + |r|^2)$, then this is the minimal polynomial. Since the minimal polynomial has the same factors as the characteristic polynomial, $p(x) = (x^2 - 2\Re(r)x + |r|^2)^k$. Since our minimal polynomial has no repeated complex root, T_a is diagonalizable over $\mathbb{C}$ (see Linear Algebra notes, 8-2).
   a. If $\mathrm{trace}(T_a) = 0$, then the eigenvalues are pure imaginary $\pm ri$, and T_a^2 is diagonalizable with eigenvalues $-r^2$. Thus $T_a^2 = -r^2 I_V \Rightarrow a^2 = -r^2 \leq 0$.
   b. Conversely, if $a^2 \leq 0$, then $T_a^2 = -r^2 I_V$ for some r, and the eigenvalues of T_a can only be $\pm ri$. Then $\mathrm{trace}(T_a) = 0$.
   c. Hence $V = \{a | \mathrm{trace}(T_a) \leq 0\}$. $T: a \to \mathrm{trace}(T_a)$ is a linear operator with range $\mathbb{R}$ (dimension 1). Since V is the kernel, V has codimension 1.
2. From (1), $D = V \oplus \mathbb{R}$. Since $V^2 = \{v^2 | v \in V\}$ gives the reals in $(-\infty, 0]$, V^4 gives the reals in $[0, \infty)$ and V generates D as an *algebra*.
3. Let $B(a,b) = \frac{-ab-ba}{2} = \frac{a^2+b^2-(a+b)^2}{2}$. From the definition of V, B is an inner product (positive definite, symmetric). Choose a minimal subspace W of V generating D as an algebra, and let $\{e_i | 1 \leq i \leq n\}$ be an orthonormal basis with respect to B. Then $\text{(i)} -e_i^2 = 1, \text{(ii)}\ e_i e_j = -e_j e_i (i \neq j)$.
   a. If $n = 0, V \cong \mathbb{R}$.
   b. If $n = 1, V \cong \mathbb{C}$. $(e_1^2 = -1)$
   c. If $n = 2, V \cong H$. (Check the relations.)
   d. If $n > 2$, then using then from (ii) $(e_1 e_2 e_n)^2 = 1 \Rightarrow e_1 e_2 e_n = \pm 1 \Rightarrow e_n = \pm e_1 e_2$. So $\mathrm{span}\{e_i | 1 \leq i \leq n-1\} \subset W$ with basis $\{e_i | 1 \leq i \leq n-1\}$ also generates D as an algebra, contradicting minimality.

Simple and Semisimple Algebras

[See group theory notes.]
[Add some stuff here.]

References

[A] Algebra by Michael Artin
[EoAA] Elements of Abstract Algebra by Richard Dean
[PftB] Proofs from the Book by Titu Andreescu and Gabriel Dospinescu
[TBGY] Abstract Algebra: The Basic Graduate Year, by Robert Ash
Wikipedia