ALGEBRA NOTES

PETER J MCNAMARA

ABSTRACT. These are notes for MAST30005 Algebra, a third year undergraduate subject taught at the University of Melbourne. Please let me know of any errors or typos you might spot. This document makes no guarantee of being comprehensive.

CONTENTS

Date: June 2, 2023.

1. Introduction

The major goal of this course is a first introduction to commutative algebra. Topics include rings, polynomials, factorisation, ideals, modules and Galois theory.

2. Rings

Definition 2.1. *A ring is a triple $(R, +, \cdot)$ where R is a set and $+$ and $\cdot$ are two binary operations $R \times R \to R$ (written $r, s \mapsto r + s$ and $(r, s) \mapsto rs$ respectively) satisfying the following axioms :*

(1) $(a + b) + c = a + (b + c)$ *for all* $a, b, c \in R$
(2) $a + b = b + a$ *for all* $a, b \in R$
(3) *there exists* $0 \in R$ *such that* $a + 0 = a$ *for all* $a \in R$
(4) *for all* $a \in R$*, there exists* $-a \in R$ *such that* $a + (-a) = 0$
(5) $a(bc) = (ab)c$ *for all* $a, b, c \in R$
(6) $ab = ba$ *for all* $a, b \in R$
(7) *there exists* $1 \in R$ *such that* $1a = a$ *for all* $a \in R$*.*
(8) $a(b + c) = ab + ac$ *for all* $a, b, c \in R$

Remark 2.2. When the binary operations $+$ and $\cdot$ are clear from the context, we omit them and just write R.

Remark 2.3. The definition as we give is not the only definition of a ring that appears in the literature. What we have defined is also known as a *commutative ring with 1.* Elsewhere in the literature you may see a definition of ring where (6) and (7) are removed, and the axiom $(a + b)c = ac + bc$ is added.

Remark 2.4. The first four axioms are equivalent to saying that $(R, +)$ is an abelian group.

Remark 2.5. These axioms have names. They are, in order: addition is associative, addition is commutative, existence of additive identity, existence of additive inverses, multiplication is associative, multiplication is commutative, existence of multiplicative identity, distributive law.

Example 2.6. *The axioms for a ring are a subset of the axioms of a field. Therefore every field is an example of a ring.*

The extra axioms in the definition of a field are

(1) $1 \neq 0$
(2) For all $x \neq 0$, there exists x^{-1} with $xx^{-1} = 1$.

Everybody agrees on what the definition of a field is.

Example 2.7. *The integers form a ring.*

Example 2.8. *The set* $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ *is a ring.*

Example 2.9. *The set* $\{a + b\sqrt[3]{2} \mid a, b \in \mathbb{Z}\}$ *is not a ring, but the set* $\{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Z}\}$ *is a ring.*

Example 2.10. *Let S be a non-zero ring, let X be a set with at least two elements. Let R be the set of functions from X to S. If we define addition and multiplication on R pointwise, then R is a ring which has two non-zero elements a and b with $ab = 0$.*

Proposition 2.11. *The elements 0 and 1 in a ring are unique.*

Proof. Suppose 1 and 1' are two multiplicative units. Then $1' = 1 \cdot 1' = 1' \cdot 1 = 1$, using the unit axiom, the commutativity of multiplication and then the unit axiom again. The proof for 0 is the same. □

Proposition 2.12. *For all $a \in R$, $a \cdot 0 = 0 \cdot a = 0$.*

Proof. We compute $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$. Cancelling (which requires the fourth axiom to justify) implies that $a \cdot 0 = 0$. □

Example 2.13. *Let R be a ring. The ring $R[x]$ is the one-variable polynomial ring with coefficients in R. Its elements are polynomials $a_0 + a_1 x + \cdots + a_n x^n$ with $a_0, \ldots, a_n \in R$.*

Warning: Every $f \in R[x]$ determines a function from R to R, which by abuse of notation is also called f. It is possible for two distinct polynomials in $R[x]$ to determine the same function. e.g. If $R = \mathbb{F}_p$ [1] , then x^p and x determine the same function, yet they are considered distinct in $\mathbb{F}_p[x]$.

Definition 2.14. *A subring of a ring R is a subset S such that*

1. *if $a, b \in S$ then $a - b \in S$*
2. $1 \in S$
3. *if $a, b \in S$ then $ab \in S$.*

Any subring of a ring is itself a ring.

3. Homomorphisms and Ideals

Definition 3.1. *Let R and S be two rings A (ring) homomorphism from R to S is a function $\varphi : R \to S$ which satisfies*

1. *$\varphi(r + s) = \varphi(r) + \varphi(s)$ for all $r, s \in R$,*
2. *$\varphi(1) = 1$,*
3. *$\varphi(rs) = \varphi(r)\varphi(s)$ for all $r, s \in R$.*

Definition 3.2. *Let R be a ring. An ideal of R is a non-empty subset $I \subset R$ such that*

1. *If $a, b \in I$ then $a + b \in I$,*
2. *If $a \in I$ and $r \in R$ then $ra \in I$.*

Exercise 3.3. *If $\{I_j\}_{j \in J}$ is a family of ideals then their intersection $\cap_{j \in J} I_j$ is an ideal.*

The below exercise also works for infinite sums, but for simplicity we state the case of two ideals.

Exercise 3.4. *If I and J are ideals, then their sum $I + J := \{i + j \mid i \in I, j \in J\}$ is an ideal.*

[1] We use $\mathbb{F}_p$ to denote the finite field of integers modulo p where p is a prime. Later (when we have developed enough theory), we will use $\mathbb{F}_q$ for the (unique) finite field with q elements, when q is a power of a prime.

Definition 3.5. *The kernel of a homomorphism $\varphi : R \to S$ is*

$$\ker(\varphi) := \{r \in R \mid \varphi(r) = 0\}.$$

The image of φ is

$$\operatorname{im}(\varphi) := \{\varphi(r) \mid r \in R\}.$$

Proposition 3.6. *The kernel of a homomorphism is an ideal and the image is a subring.*

Example 3.7. *Let $a \in R$. Then $aR := \{ar \mid r \in R\}$ is an ideal of R. It is sometimes denoted (a). Such ideals are called principal.*

Example 3.8. *Let a be an element of a ring R. Then the evaluation map $\mathrm{ev}_a : R[x] \to R$ defined by*

$$\mathrm{ev}_a\left(\sum_{i=0}^{n} r_i x^i\right) = \sum_{i=0}^{n} r_i a^i$$

is a ring homomorphism.

Proposition 3.9. *The kernel of ev_a is the principal ideal $(x-a)R[x]$.*

Proof. We prove by induction on $n = \deg g$ that if $g(x) \in \ker \mathrm{ev}_a$ then $g(x) \in (x-a)R[x]$. The $n \leq 0$ case is trivial so suppose that $n \geq 1$.

Let r_n be the leading coefficient of $g(x)$. Let $h(x) = g(x) - r_n(x-a)^n$. Then $\deg h < \deg g$ and we can easily check that $ev_a(h(x)) = 0$. So by induction we may assume that $h(x) \in (x-a)R[x]$ so $h(x) = (x-a)q(x)$. But then $g(x) = h(x) + r_n(x-a)^n = (x-a)(q(x) + r_n(x-a)^{n_1})$ so also lies in $(x-a)R[x]$. This completes the proof of the inclusion $\ker(\mathrm{ev}_a) \subset (x-a)R[x]$ and the other inclusion is trivial. □

Remark 3.10. The above result is sometimes known as the *factor theorem*: A polynomial $p(x) \in R(x)$ satisfies $p(a) = 0$ if and only if $x - a$ divides $p(x)$.

Example 3.11. *The function $\varphi : \mathbb{Z}[\sqrt{-5}] \to \mathbb{F}_2$ given by $\varphi(a + b\sqrt{-5}) = a + b \pmod 2$ is a ring homomorphism whose kernel is a non-principal ideal.*

To check that this ideal is non-principal, note that it contains $1 + \sqrt{-5}$ and 2 and these elements have no common divisor apart from ± 1 in $\mathbb{Z}[\sqrt{-5}]$.

4. Quotient Rings

Given a ring R and an ideal I, we can define the quotient ring R/I:

The simplest way to define R/I as a set is to say that it is the quotient group of $(R,+)$ by the subgroup $(I,+)$, an approach that also tells us how to do addition in the quotient ring. Explicating this, we define an equivalence relation $\sim$ on R by $a \sim b$ if $a - b \in I$.

The underlying set of the quotient ring R/I is then defined to be the set of equivalence classes of $\sim$. We denote the equivalence class of $a \in R$ by $a + I$, or maybe $\bar{a}$ or maybe just a depending on our mood. So $a + I = b + I$ by definition if $a - b \in I$.

Addition and multiplication are defined by $(a+I)+(b+I) = (a+b)+I$ and $(a+I)(b+I) = ab + I$. That these are well-defined follows from:

Lemma 4.1. *If $a \sim c$ and $b \sim d$ then $a + b \sim c + d$ and $ab \sim cd$.*

Proof. Write $x = a - c$ and $y = b - d$. Then $x, y \in I$ by definition of $\sim$.

$$ab - cd = (c + x)(d + y) - cd = cy + xd + xy$$

As I is an ideal, $cy + xd + xy \in I$, completing the proof for the product, with the addition case being easier and omitted. □

It is not hard to check that R/I is a ring.

Example 4.2. *If $R = \mathbb{Z}$ and $I = n\mathbb{Z}$, then $R/I = \mathbb{Z}/n\mathbb{Z}$ is the integers modulo n.*

Example 4.3. *Let F be a field. The quotient ring $F[x]/(x^2)$ is a two-dimensional vector space over F. The element x is nonzero and satsifies $x^2 = 0$.*

Proposition 4.4. *Let $f : R \to S$ be a ring homomorphism and I an ideal of R with $R \subset \ker f$. Then the function $\overline{f} : R/I \to S$ defined by $\overline{f}(r + I) = f(r)$ is a ring homomorphism.*

Proof. No surprises. □

Just like for groups, and vector spaces (and ...), there is a first isomorphism theorem for rings.

Definition 4.5. *A ring homomorphism is said to be an isomorphism if it is a bijection.*

If R and S are two rings for which there exists an isomorphism $\varphi : R \to S$, we say that R and S are *isomorphic* and write $R \cong S$.

There is a thought that a "better" way to define isomorphism is to say that $\varphi : R \to S$ is an isomorphism if is is a bijection and both φ and φ^{-1} are homomorphisms. This is not needed by the following proposition (the content of which is that the inverse function is automatically a homomorphism):

Proposition 4.6. *Let $\varphi : R \to S$ be an isomorphism of rings. Then $\varphi^{-1} : S \to R$ is also a ring isomorphism.*

Theorem 4.7 (First Isomorphism Theorem)**.** *Let $\varphi : R \to S$ be a ring homomorphism. Then φ induces an isomorphism*

$$R/\ker\varphi \cong \operatorname{im}\varphi.$$

Proof. From the previous proposition φ induces a ring homomorphism $\bar{\varphi} : R/\ker\varphi \to \operatorname{im}\varphi$. It is surjective by construction and injective as if $x + \ker\varphi \in \ker\bar{\varphi}$ then $\varphi(x) = \bar{\varphi}(x + I) = 0$ so $x \in \ker\varphi$ and hence $x + \ker\varphi = 0$. □

Example 4.8.

$$\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}.$$

We end with a useful criterion on when a quotient ring is a field.

Definition 4.9. *An ideal I of a ring R is maximal if $I \neq R$ and for any ideal J with $I \subset J \subset R$, either $J = I$ or $J = R$.*

Theorem 4.10. *Let I be an ideal of a ring R. Then R/I is a field if and only if I is a maximal ideal.*

5. Division

Given an integer n and a non-zero integer d, we can divide n by d to produce a quotient q and a remainder r. More precisely, we have $n = qd + r$, where $r \in \{0, 1, 2, \ldots, |d| - 1\}$. What will be important is that r is smaller than d in a precise sense.

The same also works for polynomials. We mostly use the following result when R is a field but state it in full generatlity:

Theorem 5.1. *Let R be a ring. Let $f, d \in R[x]$ be polynomials and assume d has a unit as its leading coefficient (in particular $d \neq 0$). Then there exist $q, r \in R[x]$ with $f = qd + r$ and $\deg r < \deg d$.*

In fact the q and r guaranteed to exist by this theorem are unique.

Proof. Let $X = \{f - qd \mid q \in R[x]\}$. Choose $r \in X$ of minimal degree. Suppose that $\deg r \geq \deg d$. Write $r = r_n x^n + \cdots + r_0$ and $d = d_m x^m + \cdots + d_0$. Let $s = r - r_n d_m^{-1} x^{n-m} d$. Then $s \in X$ and $\deg s < \deg r$, a contradiction. □

Remark 5.2. This is not the "standard" proof. The more common approach is to use polynomial long division, which also gives an algorithm to compute q and r.

6. Domains

Definition 6.1. *A ring is an integral domain if it is not the zero ring and whenever $ab = 0$, either $a = 0$ or $b = 0$.*

Definition 6.2. *A Euclidean domain is an integral domain R with a function $f : R\backslash\{0\} \to \mathbb{N}$ such that for all $n, d \in R$ with $d \neq 0$, we can write $n = qd + r$ with $f(r) < f(d)$ or $r = 0$.*

Definition 6.3. *A principal ideal domain is an integral domain where every ideal is principal.*

Definition 6.4. *A non-zero non-unit element r in an integral domain is irreducible if whenever $r = ab$, either a is a unit or b is a unit.*

Definition 6.5. *An element p in an integral domain is prime if p is not zero or a unit and whenever p divides ab, either p divides a or p divides b.*

Definition 6.6. *Two elements a and b are associates if there is a unit u such that $a = bu$.*

Being associates is an equivalence relation.

Definition 6.7. *A unique factorisation domain is an integral domain where every nonzero element has a factorisation into irreducibles which is unique up to associates.*

More precisely, this means that if x is a nonzero element in a unique factorisation domain R, then we can write

$$x = up_1p_2 \cdots p_n$$

with u a unit, $n \in \mathbb{N}$ and each p_i irreducible. Furthermore if we also have

$$x = vq_1q_2 \cdots q_r$$

with v a unit, $r \in \mathbb{N}$ and each q_i irreducible, then $r = n$ and there exists a permutation σ such that p_i and $q_{\sigma(i)}$ are associates for all i.

Theorem 6.8. *A Euclidean domain is a principal ideal domain.*

Proof. Let I be an ideal in a Euclidean domain R. Let d be a nonzero element of I with $f(d)$ minimal. Let $n \in I$. Then $n = qd + r$ with either $r = 0$ or $f(r) < f(d)$. Since $r \in I$, the second condition contradicts the minimality of $f(d)$, and therefore $r = 0$. Therefore $n \in dR$ so $I = dR$. □

We now define the greatest common divisor of two elements.

Definition 6.9. *Let a and b be elements of an integral domain R. A greatest common divisor d of a and b is an element of R such that*

(1) *$d \mid a$ and $d \mid b$.*
(2) *If $e \mid a$ and $e \mid b$ then $e \mid d$.*

Remark 6.10. A greatest common divisor may not exist. It always exists when R is a unique factorisation domain. When it does exist, it is unique up to associates.

Proposition 6.11. *If R is a principal ideal domain, then greatest common divisors always exist.*

Proof. The sum $aR + bR$ is an ideal (Exercise 3.4), hence is principal as R is a principal ideal domain. Let $d \in R$ be such that $aR + bR = dR$. Then d is a greatest common divisor of a and b. □

Corollary 6.12. *(Bezout's Lemma) Let R be a principal ideal domain, $a, b \in R$ and d a greatest common divisor of a and b. Then there exists $x, y \in R$ with $d = ax + by$.*

Remark 6.13. The extended Euclidean algorithm gives and algorithm to construct x and y when R is a Euclidean domain.

Proposition 6.14. *In a principal ideal domain, every irreducible element is prime.*

Proof. Let p be an irreducible element and let a and b be elements with $p \mid ab$. Assume p doesn't divide a. Then as p is irreducible, 1 is a gcd of p and a. Therefore we can write $1 = px + ay$ for some $x, y \in R$. Therefore $b = pxb + aby$ and hence $p \mid b$. □

Theorem 6.15. *Let R be a principal ideal domain and let p be irreducible. Then $R/(p)$ is a field.*

Proof. Let $a \in R/(p)$, $a \neq 0$. Lift a to an element $a \in R$. Then as p is irreducible and a is not divisible by p, the greatest common divisor of p and a is 1. Therefore by Corollary 6.12, there exists $x, y \in R$ with $1 = ax + bp$. Then x is a multiplicative inverse of a in $R/(p)$, which is enough to conclude $R/(p)$ is a field. □

Theorem 6.16. *A principal ideal domain is Noetherian.*

Proof. Let $I_1 \subset I_2 \subset \cdots$ be a chain of ideals. Let $I = \cup_{i=1}^{\infty} I_i$. Then I is an ideal. As we are in a principal ideal domain $I = (x)$ for some x. But $x \in I_n$ for some n and therefore $I = I_n$. □

Proposition 6.17. *In a Noetherian ring, every element can be factored into irreducibles.*

Proof. Proceed greedily. i.e. Factor $r = a_1a_2$. Then factor $a_1 = b_1b_2$ and $a_2 = b_3b_4$ et cetera (unless a_1 or a_2 are irreducible in which case we stop) until we have writen r as a product of irreducibles. This process terminates unless there is an infinite chain $x_1, x_2, \ldots$ for which $x_{i+1} \mid x_i$ for all i. Now consider the corresponding infinite chain of principal ideals $x_1R \subsetneq x_2R \subsetneq \cdots$. The existence of this infinite chain is impossible by the Noetherian property of R. □

Theorem 6.18. *A principal ideal domain is a unique factorisation domain.*

Proof. By Theorem 6.16, a principal ideal domain is Noetherian. Hence every element can be factored into irreducibles by Proposition 6.17.

Now suppose that $p_1 \ldots p_m = q_1 \ldots q_n$ are two factorisations of the same element into irreducibles. By Proposition 6.14, p_1 is prime. Therefore p_1 divides q_i for some i. As q_i is irreducible, p_1 and q_i are associates. Now we can divide by p_1 and proceed by induction. □

Example 6.19. *Let F be a field. Then the ring $F[x_1, x_2, \ldots]$ of polynomials in infinitely many variables is a unique factorisation domain (by Theorem 7.5 below) that is not Noetherian.*

7. Fraction Fields

In this section we give a useful construction, the field of fractions or fraction field, which generalises the construction of $\mathbb{Q}$ from $\mathbb{Z}$. This construction will be further generalised when you learn more commutative algebra/algebraic geometry (e.g. Stacks Project Tag 00CM).

Let R be an integral domain (an assumption in place throughout the whole section, unless otherwise stated). We will construct a field $\mathrm{Frac}(R)$, called the field of fractions of R, in which R embeds.

Elements of R will be fractions $\frac{a}{b}$ where $a \in R$ and $b \in R \setminus \{0\}$. We will want to say that $\frac{a}{b} = \frac{c}{d}$ whenever $ad - bc = 0$.

Proposition 7.1. *The relation $\sim$ on $R \times R$ given by $(a, b) \sim (c, d)$ if $ad = bc$ is an equivalence relation.*

Proof. The most interesting part is the transitivity. Suppose $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$. Then $adf = bcf = bde$ so cancelling gives $af = be$ as required. (note the use of the fact we're in an integral domain). □

Definition 7.2. *The field of fractions of R is the set* $\mathrm{Frac}(R)$ *of equivalence classes of $\sim$ on $R \times R$. Addition and multiplication are defined by*

$$(a, b) + (c, d) = (ad + bc, bd) \quad \textit{and} \quad (a, b) \cdot (c, d) = (ac, bd).$$

It remains to check that this is well-defined and defines the structure of a field on $\mathrm{Frac}(R)$.

We will usually use the notation $\frac{a}{b}$ instead of (a, b) to denote an element of the fraction field.

Theorem 7.3. *Let R be an integral domain. Then*

(1) *$Frac(R)$ is a field.*
(2) *$\varphi : R \to \mathrm{Frac}(R)$ defined by $\varphi(r) = \frac{r}{1}$ is an injective ring homomorphism.*

(3) *If F is a field and $f : R \to F$ is a ring homomorphism, then there exists a unique homomorphism $\iota : \mathrm{Frac}(R) \to F$ such that $f = \iota \circ \varphi$.*

Theorem 7.4 (Gauss' Lemma)**.** *Let p be a prime element in a ring R. Suppose $f, g \in R[x]$ are such that $p \mid fg$. Then $p \mid f$ or $p \mid g$.*

Proof. Suppose not. Let f_i be the smallest degree coefficient of f not divisible by p and g_j be the smallest degree coefficient of g not divisible by p. Then $p \mid f_i g_j$ which implies $p \mid f_i$ or $p \mid g_j$ as p is prime, a contradiction. □

Theorem 7.5. *Let R be a unique factorisation domain. Then $R[x]$ is a unique factorisation domain.*

Proof. Let $F = \mathrm{Frac}(R)$. Then F is a field so $F[x]$ is a unique factorisation domain. Let $f \in R[x]$ Then we can factor $f = g_1 \dots g_n$ into irreducibles in $F[x]$. Clearing denominators we have $rf = h_1 h_2 \dots h_n$ in $R[x]$. Let p be prime dividing r. By Gauss' Lemma, $p \mid h_i$ for some i. So we can divide by p to get a smaller factorisation in $R[x]$. Repeating this argument to eliminate r (note that irreducibles are prime in a UFD), we get a factorisation of f in $R[x]$ which agrees with the factorisation in $F[x]$. Since the factorisation in $F[x]$ is unique, so is the one in $R[x]$. □

8. MODULES

Modules can be thought of as the things rings naturally act on (in the way that groups act on sets), or as a generalisation of linear algebra where the coefficients are taken to lie in a ring, as opposed to lying in a field.

Definition 8.1. *Let R be a ring. An R-module $(M, +, \cdot)$ is a set M, a binary operation $+ : M \times M \to M$ (written $(m, n) \mapsto m + n$)) and a binary operation $\cdot : R \times M \to M$ (written $(r, m) \mapsto r \cdot m$ or $(r, m) \mapsto rm$ such that*

1. *$(M, +)$ is an abelian group*
2. *$1m = m$ for all $m \in M$*
3. *$(rs)m = r(sm)$ for all $r, s \in R$ and $m \in M$*
4. *$(r + s)m = rm + sm$ for all $r, s \in R$ and $m \in M$*
5. *$r(m + n) = rm + rn$ for all $r \in R$ and $m, n \in N$.*

Because of the third condition, we may unambiguously write things like rsm.

Example 8.2. *An ideal I of R is an R-module. (In fact, ideals are precisely the submodules of the R-module R).*

Example 8.3. *If F is a field, then a F-module is the same thing as a vector space.*

Example 8.4. *A $\mathbb{Z}$-module is the same thing as an abelian group.*

Example 8.5. *Let F be a field. A $F[x]$-module is the same thing as a F-vector space V, together with a linear transformation $T : V \to V$.*

Example 8.6. *Let F be a field. A $F[x, y]$-module is not the same thing as a F-vector space V, together with two linear transformations $S, T : V \to V$, because linear transformations do* *not commute. It is the same thing as a F-vector space V together with two commuting linear transformations $S, T : V \to V$.*

Definition 8.7. *Let A and B be two R-modules. Their direct sum is*

$$A \oplus B = \{(a, b) \mid a \in A, b \in B\}$$

where $(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$ and $r(a, b) = (ra, rb)$.

Definition 8.8. *Let M and N be two R-modules. A homomorphism from M to N is a function $\varphi : M \to N$ which satisfies*

(1) *$\varphi(m + n) = \varphi(m) + \varphi(n)$ for all $m, n \in M$.*
(2) *$\varphi(rm) = r\varphi(m)$ for all $r \in R$ and $m \in M$.*

Definition 8.9. *A submodule of an R-module M is a subset $N \subset M$ such that*

(1) *$0 \in N$,*
(2) *If $n_1, n_2 \in N$ then $n_1 + n_2 \in N$,*
(3) *If $n \in N$ and $r \in R$ then $rn \in N$.*

A submodule of an R-module is an R-module in its own right.

Example 8.10. *Let R be an interal domain and let M be an R-module. Then*

$$M_{\text{tors}} = \{m \in M \mid \text{there exists } r \in R \setminus \{0\} \text{ such that } rm = 0\}$$

is a submodule of M. It is called the torsion submodule of M and elements inside it are called torsion elements.

Proposition 8.11. *Let M be a R-module. Suppose that A and B are two submodules such that $A \cap B = \{0\}$ and $A + B = M$. Then $M \cong A \oplus B$.*

Proof. Define a homomorphism $\varphi : A \oplus B \to M$ by $\varphi(a, b) = a + b$. It is surjective since $A + B = M$ and it is injective since $A \cap B = \{0\}$. □

Proposition 8.12. *Let $\pi : M \to F$ be a surjective homomorphism with F free. Then there exists $s : F \to M$ with $\pi \circ s = id_F$.*

Remark 8.13. This is sometimes referred to as "free modules are projective", since this property being ascertained about F is one definition of being a projective module. We won't have any further reasons to talk about projective modules in this course, but they play a pivotal role in homological algebra later on.

Proof. Let $\mathcal{B}$ be a basis of F. For each $b \in \mathcal{B}$, choose $s(b) \in f^{-1}(b)$. This extends uniquely to a desired homomorphism $s : F \to M$. □

9. Noetherian Modules

This is a technical section on finiteness properties for modules needed in order to prove Theorem 11.3. It can be skipped until needed. It contains a proof of the fact that a subgroup of a finitely generated abelian group is finitely generated. (the corresponding statement with the word abelian removed is false).

Definition 9.1. *Let M be an R-module. Then M is Noetherian if every ascending chain of ideals stabilises.*

Theorem 9.2. *Let R be a Noetherian ring. Then any finitely generated R-module is Noetherian.*

Corollary 9.3. *Let R be a Noetherian ring. Then any submodule of a finitely generated R-module is finitely generated.*

10. Presentation Matrices

Let M be a R-module. Let $\{m_i\}_{i \in I}$ be a generating set for M. Define $\psi : R^I \to M$ by $\psi((r_i)) = \sum_i r_i m_i$. Then ψ is surjective.

We now perform the same construction to $\ker \psi$, to obtain a surjective homomorphism $\varphi : R^J \to \ker \psi$. Consider the composition, which by abuse of notation we'll also call φ:

$$\varphi : R^J \twoheadrightarrow \ker \psi \hookrightarrow R^I.$$

The homomorphism $\varphi : R^J \to R^I$ can be expressed by a matrix Φ with entries in R (just like in traditional linear algebra). Such a matrix is called a *p*resentation matrix for M. Note, this matrix is very far from being unique.

The module M can be reconstructed from a presentation matrix φ as $M \cong \operatorname{coker} \varphi$. (the cokernel of $f : M \to N$ is defined to be $\operatorname{coker} f = N / \operatorname{im} f$).

10.1. Generators and Relations.

There is another way to think about presentation matrices in terms of generators and relations.

Theorem 10.1. *Let Φ be a presentation matrix for a module M as constructed above. Then M is generated by elements $\{m_i\}_{i \in I}$ subject to one relation from each column of Φ, namely $\sum_i \Phi_{ij} m_i = 0$.*

To say that a module M is given by generators $\{m_i\}$ subject to some relations means that the elements $\{m_i\}$ generate M and that every identity that holds in M can be decuded from the given set of relations.

Lemma 10.2. *Let $\pi : A \to B$ and $\varphi : C \to D$ be two R-module homomorphisms. Suppose that there exist isomorphisms $f : A \to C$ and $g : B \to D$ such that $\varphi \circ f = g \circ \pi$. Then* $\operatorname{coker} \pi \cong \operatorname{coker} \varphi$.

11. Smith Normal Form

Theorem 11.1 (Smith Normal Form)**.** *Let R be a principal ideal domain. Let $X \in Mat_{m \times n}(R)$. Then there exists $A \in GL_m(R)$ and $B \in GL_n(R)$ such that the only nonzero elements of AXB are on the main diagonal, and if $d_1, d_2, \ldots, d_{\min(m,n)}$ denote these elements, then $d_i \mid d_{i+1}$ for all i.*

Proof. We will say that $X \sim X'$ if there exists $A \in GL_m(R)$ and $B \in GL_n(R)$ with $X' = AXB$. Let x_{ij} denote the entry of X in the (i, j)-th position.

Suppose that $x_{11} \nmid x_{1j}$ for some $j > 1$. Let $e = \gcd(x_{11}, x_{1j})$. Then $e \neq 0$ (if $e = 0$ then $x_{11} = x_{1j} = 0$ which contradicts our assumption).

Then as R is a PID, there exists $a, b \in R$ with $e = ax_{11} + bx_{1j}$ Let $B = (b_{kl})$ be the $n \times n$ matrix with $b_{11} = a$, $b_{j1} = b$, $b_{1j} = -x_{1j}/e$, $b_{jj} = -x_{11}/e$, $b_{kk} = 1$ if $k \neq 1, j$ and all other entries are zero. Then $\det(B) = 1$ so $B \in GL_n(R)$. Let $X' = XB$. Then $x'_{11} = e$ is a proper divisor of x_{11} and $x'_{11} \mid x'_{1j}$.

There is a similar construction we can do if x_{11} does not divide an entry in the same column. □

If R is a Euclidean domain, there is a stronger version of Smith Normal Form:

Theorem 11.2. *(SNF for a Euclidean domain) Let R be a Euclidean domain. Let X be a matrix with entries in R. Then after applying row and column operations, it is possible to turn X into a matrix whose only nonzero entries are along the diagonal, $d_1, d_2, \ldots$ and satisfy $d_1 \mid d_2 \mid \cdots$*

Theorem 11.3. *Let R be a principal ideal domain. Let M be an R-module and let A be a presentation matrix of M. Then*

$$M \cong R/(d_1) \oplus R/(d_2) \oplus \cdots \oplus R/(d_m)$$

where the Smith Normal form of A has diagonal entries $d_1, \ldots, d_{\min(m,n)}$ and $d_i = 0$ if $i > \min(m, n)$.

Proof. The major part of the proof is Theorem 11.1. We also need Lemma 10.2, Theorem 6.16 and §9 to finish. □

When $R = \mathbb{Z}$, we obtain the classification of abelian groups.

Theorem 11.4. *Let F be a field and C be a finite subgroup of $F^\times$. Then C is cyclic.*

Proof. By the classification theorem for abelian groups, either C is cyclic or there exists $n < |C|$ with $x^n = 1$ for all $x \in C$. The latter cannot occur since a polynomial over a field cannot have more roots than its degree. □

Remark 11.5. This theorem subsumes the classical result in number theory that a primitive root exists modulo every prime.

When $R = k[x]$ when k is an algebraically closed field, we obtain Jordan normal form.
When $R = k[x]$ where k is a field, we obtain the rational canonical form.

12. Irreducibility of Polynomials

One frequently wants to know when single variable polynomials over a field are irreducible (c.f. the following sections where they are used to construct field extensions). Here we present a couple of techniques.

Theorem 12.1. *Let R be a unique factorisation domain and let $F = \mathrm{Frac}(R)$. If $f(x) \in R[x]$ is irreducible, then $f(x)$ is irreducible in $F[x]$*

Proof. This follows from Gauss' Lemma (Theorem 7.4). □

It is common to use this result to turn questions about irreducibility in $F[x]$ into questions about irreducibility in $R[x]$, where we have more techniques at our disposal, in particular reducing modulo an ideal. Sometimes the techniques of proof in the below are more important and more applicable than the statements.

Theorem 12.2. *Let R be a ring and I an ideal of R. Let $f(x) \in R[x]$ be monic. If $f(x)$ is irreducible in $(R/I)[x]$, then $f(x)$ is irreducible in $R[x]$.*

Theorem 12.3. *(Eisenstein's criterion) Let R be an integral domain. Let $f(x) = \sum_{i=0}^{n} a_n x^n \in R[x]$ be a polynomial such that there exists a prime $p \in R$ with $p \nmid a_n$, $p \mid a_i$ for all $i < n$ and $p^2 \nmid a_0$. If $f(x) = g(x)h(x)$ for $g(x), h(x) \in R[x]$, then either $g(x)$ or $h(x)$ is constant.*

Proof. Look at the lowest degree coefficients of $g(x)$ and $h(x)$ which are not divisible by p. They multiply to give the lowest degree coefficient of $f(x)$ which is not divisible by p (since p is prime). Since the only coefficient of $f(x)$ which is not divisible by p is the leading one, each of $g(x)$ and $h(x)$ can only have their leading coefficient not divisible by p. So if $g(x)$ and $h(x)$ are both of positive degree, their constant terms are both divisible by p, which contradicts $p^2 \nmid a_0$. □

Remark 12.4. There is a version where primes are replaced by prime ideals. We shan't need that version in this course.

Remark 12.5. Eisenstein's criterion is generalised using Newton polygons (one keyword: p-adic numbers), which is really all about keeping track of what powers of p appear everywhere.

Example 12.6. *Let p be a prime. Then the polynomial*

$$\frac{x^p - 1}{x - 1}$$

is irreducible over $\mathbb{Q}$.

Proof. Make the substitution $x = y + 1$ and apply Eisenstein's criterion. □

Remark 12.7. This example is generalised in §21.

13. Field Extensions

If F is a subfield of a field K, then we say that K is a field extension of F. Sometimes we write K/F to talk about a field extensions, this is just a piece of notation which means"over F", and does not indicate a quotient.

Definition 13.1. *If K/F is a field extension and $\alpha \in K$, then we say α is algebraic over F if α is the root of a nonzero polynomial with coefficients in F. Otherwise we say α is trancendental.*

For example $2\pi i$ is algebraic over $\mathbb{R}$ and trancendental over $\mathbb{Q}$. The former is because $2\pi i$ is a root of the polynomial $x^2 + 4\pi$ while the latter fact is a famous theorem.

With notation as above, we let $F[\alpha]$ be the smallest subring of K containing F and α, and let $F(\alpha)$ be the smallest subfield of K containing F and α.

There is always a unique homomorphism $F[x] \to K$ sending x to α. Its image is $F[\alpha]$. Its kernel is trivial if α is trancendental, otherwise it is a principal ideal generated by a monic polynomial $m(x)$. This is the smallest degree monic polynomial which has α as a root and is called the *minimal polynomial* of α (over F). The degree of α is defined to be the degree of this polynomial.

The following is immediate and rather useful:

Proposition 13.2. *Let K/F be a field extension and let $\alpha \in K$. Let $m(x)$ be the minimal polynomial of α. Then for $f \in F[x]$, $f(\alpha) = 0$ if and only if $m(x) \mid f(x)$.*

The following is very useful.

Theorem 13.3. *Let F be a field and $p(x) \in F[x]$ be a polynomial of degree $d \geq 0$. Then*

$$\dim_F \left(F[x]/(p(x))\right) = d.$$

Proof. We prove this by showing that $1, x, x^2, \ldots, x^{d-1}$ form a basis.

To show they span, let $f \in F[x]$. Then by the division algorithm, we can write $f = pq + r$ with $\deg(r) < d$. Therefore $f = r$ in $F[x]/(p(x)$. Since $\deg(r) < d$, the element r is in the span of $1, x, x^2, \ldots, x^{d-1}$ and therefore f is as well.

Now to show they are linearly independent, suppose $a_0 + a_1 x + \cdots + a_{n-1}x^{d-1} = 0$. Write $a(x)$ for this polynomial. Then $p(x) \mid a(x)$. Since $\deg(a) < \deg(p)$, the only way this is possible is if $a(x) = 0$, implying $a_i = 0$ for all i as required. □

Theorem 13.4. *Let K/F be a field extension and $\alpha \in K$. Then α is algebraic over F if and only if $F[\alpha]$ is a field.*

Proof. Suppose α is algebraic over F (the other direction is straightforward). Consider the canonical homomorphism $\varphi : F[x] \to K$ defined by $\varphi(x) = \alpha$. Consider the ideal $\ker \varphi$. It is a principal ideal since $F[x]$ is a principal ideal domain. Let $d(x)$ be a generator of this ideal. Since α is assumed to be algebraic, $d(x) \neq 0$. The first isomorphism theorem shows that $F[x]/(d(x)) \cong F[\alpha]$. Since $F[\alpha]$ is a subring of a field, it is an integral domain. Therefore $d(x)$ is irreducible. By Theorem 6.15, $F[x]/(d(x))$ is a field. □

Definition 13.5. *The degree of a field extension K/F, denoted $[K : F]$ is defined to be the dimension of K as a F-vector space.*

For example, the degree of α is equal to $[F[\alpha] : F]$.

If the degree is finite, we say that K/F is a finite extension.

Proposition 13.6. *If K/F is a finite field extension, then every element of K is algebraic over F.*

Proof. Let $d = [K : F]$. Then for all $\alpha \in K$, the set $\{1, \alpha, \alpha^2, \ldots, \alpha^d\}$ has $d+1$ elements thus is linearly dependent over F. □

Proposition 13.7. *Let K be a field extension of F and L be a field extension of K. Then $[L : F] = [L : K][K : F]$.*

Proof. Let a_i be a basis of L over K. Let b_j be a basis of K over F. Consider the set of products $\{a_i b_j\}$. We will show this set is a basis of L over F.

Let $x \in L$. Then there exists $k_i \in K$ with $x = \sum_i k_i a_i$. For each i there exists $c_{ij} \in F$ with $k_i = \sum_j c_{ij} b_j$. Then $x = \sum_{i,j} c_{ij} a_i b_j$ so this is a spanning set.

Suppose $c_{ij} \in F$ are such that $\sum_{ij} c_{ij} a_i b_j = 0$. Write this as $\sum_i (\sum_j c_{ij} b_j) a_i = 0$. As the a_i are linearly independent over K, we get $\sum_j c_{ij} b_j = 0$ for all j. As the b_j are linearly independent over F, we get $c_{ij} = 0$ for all i, j, as required. □

Remark 13.8. The above result and proof work whether or not the extensions involved are finite.

Let K be a field extension of F. Define K_{alg} to be the subset of all algebraic elements of K.

Definition 13.9. *A field is algebraically closed if every nonconstant polynomial has a root.*

Example 13.10. *The field of complex numbers is algebraically closed. A proof is given in Section 18.*

Theorem 13.11. *Let K be a field extension of F. Then K_{alg} is a field. If K is algebraically closed, then K_{alg} is algebraically closed.*

Proof. Let α and β be in K_{alg}. From Theorem 13.4, it suffices to show that $\alpha+\beta$ and $\alpha\beta$ are in K_{alg}. As β is algebraic over F, it is algebraic over $F[\alpha]$. Therefore $F[\alpha, \beta]$ is finite over F. As $\alpha+\beta$ and $\alpha\beta$ are in $F[\alpha, \beta]$ which is a finite extension of F, they are algebraic over F, which finishes the proof that K_{alg} is a field.

Now assume K is algebraically closed. Suppose that $f(x) = \sum_{a_i} x^i \in K_{\text{alg}}[x]$ and $z \in K$ is such that $f(z) = 0$. Then z is algebraic over $F[\alpha_0, \dots, a_n]$ which is finite over F, therefore z lives in a finite extension of F, therefore $z \in K_{\text{alg}}$ which prove that K_{alg} is algebraically closed. □

Definition 13.12. *Let R be a ring and $f(x) = \sum_{i=0}^n a_i x^i \in R[x]$. Its derivative is defined to be*

$$f'(x) = \sum_{i=1}^n i a_i x^{i-1}.$$

Theorem 13.13. *The derivative satisfies the usual product and sum rules from calculus:*

$$(f+g)' = f' + g' \qquad (fg)' = f(g') + (f')g.$$

Proof. We show one way to deduce this theorem from the usual sum and product rules from calculus (A more boring proof exists, where you just expand everything out using the definitions, but lets pretend we don't see that and continue). Let $f(x) = \sum_{i=0}^n a_i x^i$ and $g(x) = \sum_{j=0}^m b_j x^j$. Expanding out $(fg)'$ from the definition, the coefficient of x^k is some polynomial $F(a_0, \dots, a_n, b_0, \dots, b_m)$. Expanding out $f(g')+(f')g$, the coefficient of x^k is some polynomial $G(a_0, \dots, a_n, b_0, \dots, b_m)$. The polynomials F and G have integer coefficients and do not depend on the ring R, which can now be safely forgotten about.

We rely on the following standard fact (which you should be able to prove): If two polynomials with integer coefficients $F(x_1, \dots, x_n)$ and $G(x_1, \dots, x_n)$ are the same when evaluated at all points of $\mathbb{R}^n$, then they are identical polynomials. (Bonus useless paranthetical fact: there exists a single point in $\mathbb{R}^n$ at which equality of the evaluations implies equality of the polynomials!).

Once we have this fact, we may say without loss of generality that $R = \mathbb{R}$ in which case the desired equality follows from the fact that we have defined the derivative to agree with that from calculus when $R = \mathbb{R}$, together with the product rule in calculus. □

Definition 13.14. *If K is a field and $f \in K[x]$, we say that $\alpha \in K$ is a double root of f if $(x-\alpha)^2 \mid f$.*

Theorem 13.15. *Let F be a field and $f \in F[x]$. Then there exists a field extension K/F in which F has a double root if and only if* $\gcd(f, f') \neq 1$.

Proof. If F has a double root α in K, then $f = (x-\alpha)^2 g$ for some $g \in K[x]$. Then $f' = (x-\alpha)^2 g' + 2(x-\alpha)g$, so $x - \alpha$ is a common factor of f and f', implying their gcd is not 1.

Conversely, suppose $\gcd(f, f') \neq 1$. Let d be a nontrivial common divisor of f and f'. Let K be a field extension in which d has a root α. Then $x-\alpha$ divides d, hence divides f and f' in $K[x]$. Write $f = (x-\alpha)g$. Then $f' = g + (x-\alpha)g'$, so as $x - \alpha$ divides f', it must divide g. Therefore $(x-\alpha)^2$ divides f as required. □

Proposition 13.16. *If F is a field of characteristic zero and $f \in F[x]$ is irreducible, then* $\gcd(f, f') = 1$.

Proof. Since F has characteristic zero, $f' \neq 0$. Since $\deg(f') < \deg(f)$, $\gcd(f, f')$ is a proper divisor of f, hence is constant as f is irrecucible. □

Corollary 13.17. *If F is a field of characteristic zero and $f \in F[x]$ is irreducible, then f has no double roots in any field extension of F.*

Example 13.18. *If F is of characteristic $p > 0$, it is possible for an irreducible polynomial to have vanishing derivative. For example if $F = \mathbf{F}_p(t)$ and $f(x) = x^p - t$. This polynomial has a root of multiplicity p in the extension $F(t^{1/p})$ as over this field, $f(x) = (x - t^{1/p})^p$.*

14. Galois Groups

Definition 14.1. *Let K/F be a field extension. A F-automorphism of K is an isomorphism $\sigma : K \to K$ which is the identity when restricted to F.*

Example 14.2. *Complex conjugation is a $\mathbb{R}$-automorphism of $\mathbb{C}$. Complex conjugation is not a $\mathbb{Q}[i]$-automorphism of $\mathbb{C}$.*

Example 14.3. *The field extension $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ has no automorphisms apart from the identity.*

To prove this, suppose $\sigma : \mathbb{Q}[\sqrt[3]{2}] \to \mathbb{Q}[\sqrt[3]{2}]$ is an automorphism. Then $(\sigma(\sqrt[3]{2}))^3 - 2 = 0$. If $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$, then σ is the identity, as $\sqrt[3]{2}$ generates the field extension. So it must be that $\sigma(\sqrt[3]{2}) = \zeta\sqrt[3]{2}$ for some nontrivial third root of unity ζ (we do this computation in $\mathbb{C}$). For σ to be an automorphism requires $\zeta \in \mathbb{Q}[\sqrt[3]{2}]$. But $\zeta \notin \mathbb{R}$ and $\mathbb{Q}[\sqrt[3]{2}] \subset \mathbb{R}$, a contradiciton.

This example shows a general philosophy that we can constrain field automorphisms by looking at how they behave on generators. What is so far missing is how to construct field automorphisms. One method is by the following theorem:

Theorem 14.4. *Let F be a field, $f \in F[x]$ be irreducible and $K = F[x]/(f)$. If α and β are two roots of f in K, then there is a unique F-automorphism of K sending α to β.*

Proof. Construct isomorphisms from $F[x]/(f)$ to K sending x to α and β respctively. □

Example 14.5. *If p is prime and $\zeta = e^{2\pi i/p}$, then for every integer d not divisible by p, there is an automorphism σ of $\mathbb{Q}[\zeta]$ with $\sigma(\zeta) = \zeta^d$.*

Remark 14.6. This produces $p-1$ automorphisms of $\mathbb{Q}[\zeta]$ (which is all of them - to prove there are no more, note that if σ is an automorphism, it is completely determined by where it sends ζ. Existence is discussed below) Under composition they form a group which is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\times$ (which is non-canonically cyclic of order $p-1$). This example generalises to the extension field of $\mathbb{Q}$ generated by any root of unity. (The statement is that if ζ is a primitive n-th root of 1, then $\mathbb{Q}[\zeta]$ is Galois over $\mathbb{Q}$ with Galois group $(\mathbb{Z}/n\mathbb{Z})^\times$).)

The existence of these automorphisms follows from Theorem 14.4 applied to $f(x) = \frac{x^p-1}{x-1}$, noting that ζ and ζ^d are both roots of f. Note the irreducibility of $f(x)$ was discussed in Example 12.6.

Theorem 14.7. *Let K be a field and G a finite group of automorphisms of K. Then $[K : K^G] = |G|$.*

Proof. Let $n = |G|$. Let $a_0, a_1, \dots, a_n \in K$ be $n+1$ elements of K. Consider the system of n equations,

$$\sum_{i=0}^{n} x_i \sigma(a_i) = 0,$$

one equation for each $\sigma \in G$. Let V be the set of tuples $(x_0, \dots, x_n)$ satisfying these equations.

Since there are more variables than equations, there exists a nonzero element of V. Let $(x_0, \dots, x_n)$ be a nonzero element of V with a minimal number of nonzero entries. As V is a K-vector space, without loss of generality $x_0 = 1$. For any $g \in G$, he element

$$(0, x_1 - g(x_1), x_2 - g(x_2), \dots, x_n - g(x_n))$$

also lies in V. By our minimality assumption it must be zero. Therefore $g(x_i) = x_i$ for all i and all $g \in G$. Therefore each x_i is in K^G. Taking σ to be the identity shows that the elements a_i are linearly dependent over K^G. Since we've shown every set of $n+1$ elements is linearly dependent, $[K : K^G] \leq n$.

Now let $G = \{\sigma_1, \dots, \sigma_n\}$ and let us consider the system of equations

$$\sum_{i=1}^{n} y_i \sigma_i(x) = 0 \qquad \text{for all } x \in K. \tag{14.1}$$

Note that if we let x run over a K^G-basis of K, then we get a linear system, the solution of which implies we get a solution to (14.1). So if $[K : K^G] < n$, then there is always a nontrivial solution.

Now suppose that we have a non-trivial solution $(y_1, \dots, y_n)$ to (14.1) and choose that solution to have as few nonzero terms as possible.

If the solution has one nonzero term, then it reduces to $y_i \sigma_i(x) = 0$ with $y_i \neq 0$, which forces $x = 0$ which is absurd so cannot happen. So suppose that without loss of generality y_1 and y_2 are nonzero. Let $z \in K$ be an element with $\sigma_1(z) \neq \sigma_2(z)$

The element

$$\sigma_1(z)(y_1,\dots,y_n)-(\sigma_1(z)y_1,\sigma_2(z)y_2,\dots,\sigma_n(z)y_n)$$

is also a solution to (14.1). Since $(\sigma_1(z)-\sigma_2(z))y_2\neq 0$, this contradicts our minimality assumption. Therefore no nontrivial solution to (14.1) can exist and hence $[K:K^G]\geq n$.

The two inequalities we have proved together provide a proof of this theorem. □

15. Separability

Definition 15.1. *A field extension K/F is separable if for all $\alpha\in K$ algebraic over F with minimial polynomial $f(x)$, we have $f'(x)\neq 0$.*

The condition $f'(x)\neq 0$ is equivalent to f not having a multiple root in any field extension, and is always true when F has characteristic zero.

The standard example of an inseparable field extension is $K=F[x]/(x^p-t)$ where $t\in F$ is an element with no p-th root in F and F is a field of characteristic p.

Theorem 15.2. *(Primitive Element Theorem) Let K/F be a finite separable extension. Then there exists $\alpha\in F$ with $K=F[\alpha]$.*

Proof. If F is finite, then we can take α to be a generator of the cyclic group $K^\times$ (see Theorem 11.4 for the proof that $K^\times$ is cyclic). For the rest of the proof, suppose that K is infinite.

First suppose that $K=F[\alpha,\beta]$. Let $f(x)$ and $g(x)$ be the minimal polynomials of α and β respectively in $F[x]$. Let L be an extension field in which f and g split into linear factors. In $L[x]$, suppose

$$f(x)=\prod_{i=1}^{n}(x-\alpha_i)\qquad\text{and}\qquad g(x)=\prod_{j=1}^{m}(x-\beta_j).$$

Choose $t\in F$ such that the mn numbers $\alpha_i+t\beta_j$ are all distinct. This is possible since F is infinite and K/F is separable, which implies that $\alpha_1,\dots,\alpha_n$ are distinct, and that $\beta_1,\dots,\beta_m$ are distinct. Let $\gamma=\alpha+t\beta$. We will show that $K=F[\gamma]$.

Consider the polynomial $h(x)=f(\gamma-tx)$. Then $h(\beta)=0$ so h and g have a common factor. Suppose $h(\beta_j)=0$. Then $f(\gamma-t\beta_j)=0$ and hence $\gamma-t\beta_j=\alpha_i$ for some i. Since the numbers $\alpha_i+t\beta_j$ are all distinct, the only solution is $\alpha_i=\alpha$ and $\beta_i=\beta$.

Therefore β is the only common root of g and h in L and hence $\gcd(h,g)=x-\beta$. Both h and g are in $F[\gamma][x]$. Since the gcd is the same whether or not the computation is performed in $L[x]$ or $F[\gamma][x]$, we deduce that $\beta\in F[\gamma]$. Since $\alpha=\gamma-t\beta$, we also get $\alpha\in F[\gamma]$.

Therefore $K=F[\alpha,\beta]\subset F[\gamma]\subset K$. Hence all inclusions are equalities and we've shown $K=F[\gamma]$ as required.

This concludes the argument when K is genereated by two elements and F is infinite. An induction on the number of generators then proves the general case when F is infinte. □

16. Normal and Galois Extensions

From hereon out, we will occasionally only prove results in characteristic zero. We will endeavour to ensure that the statements made are true without this restriction, we make this assumption at times in order to avoid technical discussions on separability that otherwise will appear within proofs. I believe the Stacks Project is a reliable source that covers all the details with no restrictions on the characteristic.

Definition 16.1. *A finite field extension K/F is normal if every irreducible polynomial in $F[x]$ which has a root in K splits in K.*

Lemma 16.2. *Let $K/E/F$ be a tower of finite field extensions. If K/F is normal then K/E is normal.*

Proof. Let $f(x) \in E[x]$ be an irreducible polynomial with a root $\alpha \in K$. Let $g(x) \in F[x]$ be the minimal polynomial of α over F. Then $f(x) \mid g(x)$. Since K/F is normal, g splits into linear factors in $K[x]$, and hence so does f, as it is a divisor of g. Therefore K/E is normal. □

Proposition 16.3. *Let K/F be a splitting field of a polynomial $f(x) \in F[x]$. Then K is a normal extension of F.*

Proof. Let $g(x) \in F[x]$ be irreducible and suppose $\beta \in K$ is a root of g. We have to show that g splits into linear factors in $K[x]$.

Let $\alpha_1, \dots, \alpha_n$ be the roots (with multiplicity) of $f(x)$. As K is a splitting field for f, $K = F[\alpha_1, \dots, \alpha_n]$. Therefore there exists a polynomial h such that $\beta = h(\alpha_1, \dots, \alpha_n)$. Define the polynomial

$$p(x) = \prod_{\sigma \in S_n} \big(x - h(a_{\sigma(1)}, a_{\sigma(2)}, \dots, a_{\sigma(n)})\big)$$

The coefficients of p are symmetric polynomials in $\alpha_1, \dots, \alpha_n$, hence are polynomials in the elementary symmetric functions of $\alpha_1, \dots, \alpha_n$, hence are polynomials in the coefficients of $f(x)$. As $f(x) \in F[x]$, this implies $p(x) \in F[x]$.

As $p(\beta) = 0$ and g is the minimal polynomial of β, $g \mid p$. As p splits over K, this implies g splits over K, as required. □

Theorem 16.4. *Let K/F be a finite field extension. The following are equivalent*

1. *$|\operatorname{Aut}_F(K)| = [K : F]$,*
2. *$F = K^{\operatorname{Aut}_F(K)}$,*
3. *K/F is normal and separable,*
4. *K/F is the splitting field of a separable polynomial over F.*

Definition 16.5. *If a finite field extension K/F satisfies the conditions of the above theorem, we say it is Galois. The Galois group of K/F is then defined to be $\operatorname{Gal}_F(K) = \operatorname{Aut}_F(K)$.*

We will only give a complete proof when the fields involved are of characteristic zero, which means we can ignore all of the separability hypotheses.

Proof. The equivalence of (1) and (2) is by Theorem 14.7. The implication (4) implies (3) is Proposition 16.3. We next show that (3) implies (1).

Let K/F be a normal separable extension. By the primitive element theorem, there exists $\alpha \in K$ with $K = F[\alpha]$. Let f be the minimal polynomial of α over F. Since K is normal, F splits over K.

Let $n = [K : F]$. Then $n = \deg(f)$ and f has n roots in K. By Theorem 14.4, for each root α' of f, there exists an automorphism of K sending α to α'.

Therefore $|\operatorname{Aut}(K/F)| \geq n$. The other inequality is straightforward as every automorphism is completely determined by its value on α, and must send α to another root of f. This completes the proof that (3) implies (1).

We now show that (1) implies (4). By the primitive element theorem, there exists $\alpha \in K$ with $K = F[\alpha]$. Let f be the minimal polynomial of α over F. Let $n = [K : F]$. Then $n = \deg(f)$ and $|\operatorname{Aut}(K/F)| = n$ by assumption.

For each $\sigma \in \operatorname{Aut}(K/F)$, $\sigma(\alpha)$ is a root of f. The elements $\sigma(\alpha)$ are all distinct as α generates K. Therefore we have shown that f has n roots in K. As $n = \deg(f)$, this implies that K is a splitting field for f, completing the proof. □

The following is the main theorem of Galois Theory. Let K/F be a Galois field extension with $G = \operatorname{Gal}(K/F)$. To a subgroup H of G, we can associate an intermediate field $E = K^H$. To an intermediate field E, we can associate a subgoup $\operatorname{Aut}_E(K)$ of G. The main theorem of Galois theory says that these two operations are inverse to each other.

Theorem 16.6. *(Main Theorem of Galois Theory) Let K/F be a Galois extension with Galois group G. Then there is an inclusion-reversing bijection between intermediate fields E and subgroups of H. This bijection sends an intermediate field E to the subgroup $Aut(K/E)$ and a subgroup H to the fixed field K^H.*

Proof. Let H be a subgroup of G. The corresponding intermediate field is $E = K^H$. We have to show that $\operatorname{Aut}_E(K) = H$. Note that there is a canonical inclusion $H \subset \operatorname{Aut}_E(K)$. Note that K/E satisfies condition (2) of Theorem 16.4, hence satisfies condition (1), i.e. $|\operatorname{Aut}_E(K)| = [K : E]$, which is known to equal $|H|$ by Theorem 14.7. Hence the inclusion $H \subset \operatorname{Aut}_E(K)$ must be an equality.

Now, let E be an intermediate field. We have to show that $K^{\operatorname{Aut}_E(K)} = E$. Since K is a Galois extension of F, the field K is normal and separable over F, hence by Lemma 16.2, K is normal and separable over E. The implication (3) implies (2) of Theorem 16.4 provides the desired conclusion.

These paragraphs show that the two functions from intermediate fields to subgroups and vice versa are inverses. □

Lemma 16.7. *Let E be a finite field extension of F and K a field extension of F. Then there are at most $[E : F]$ distinct injections of fields $E \hookrightarrow K$ that fix F.*

Remark 16.8. Equality is satisfied when K is sufficiently large over F, in particular when K contains a subfield K' which is Galois over F and K' contains a subfield isomorphic to E. Given E/F, a necessary and sufficient condition for such a field K to exist is that E/F is separable.

For simplicity, we only prove this under the additional assumption when E/F is separable.

Proof. By the primitive element theorem, write $E = F[\gamma]$. Let $f(x) \in F[x]$ be the minimal polynomial of γ. Let $n = [E : F]$ be its degree. If $\sigma : E \to K$ is a field homomorphism fixing F then σ is completely determined by $\sigma(\gamma)$. As $\sigma(\gamma)$ is a root of $f(x)$ which has degree n, there are at most n choices. □

Theorem 16.9. *Let K/F be a finite Galois field extension with $G = \mathrm{Gal}(K/F)$. Let E be an intermediate field and $H = \mathrm{Gal}(K/E)$ its corresponding subgroup of G. Then E/F is Galois if and only if H is normal. Furthermore if this is the case, then $\mathrm{Gal}(E/F) = G/H$.*

Proof. First suppose E/F is Galois. Each of the $[E : F]$ elements of $\mathrm{Gal}_F(E)$ gives a different embedding of E into E (and hence into K). So by Lemma 16.7, there are no more field embeddings of E into K. Now let $\sigma \in \mathrm{Gal}_F(K)$. Then $e \mapsto \sigma(e)$ is a field embedding of E into K. Therefore it must be one of the ones already found, so the image of σ is E. Restricting to σ therefore defines for us a group homomorphism $\varphi : \mathrm{Gal}_F(K) \to \mathrm{Gal}_F(E)$. Its kernel is $\mathrm{Aut}_E(K) = \mathrm{Gal}_E(K)$ which is therefore a normal subgroup of $\mathrm{Gal}_F(K)$.

Conversely suppose that H is a normal subgroup of G. Let $\sigma \in G$ and $e \in E$. Let $h \in H$. Then

$$h(\sigma(e)) = \sigma(\sigma^{-1}h\sigma)(e) = \sigma(e),$$

the last equality being because H is normal, so $\sigma^{-1}h\sigma \in H$, which fixes E. Since E is the fixed field of H, this implies that $\sigma(e) \in E$. Therefore restriction to H defines a group homomorphism $\varphi : \mathrm{Gal}_F(K) \to \mathrm{Aut}_F(E)$. The kernel again is H, so we have an injection $G/H \hookrightarrow \mathrm{Aut}_F(E)$. Therefore $|\mathrm{Aut}_F(E)| \geq |G/H| = [E : F]$, so E/F is Galois.

In the course of the proof, we also saw that $\mathrm{Gal}_F(E) \cong G/H$.

□

17. Examples

Lemma 17.1. *Let p be a prime. Let G be a transitive subgroup of S_p that contains a transposition. Then $G = S_p$.*

Proof. Construct a graph on $\{1, 2, \ldots, p\}$ where vertices i and j are joined by an edge if $(ij) \in G$. Since $(ij)(jk)(ij) = (ik)$ and G is a subgroup, the graph is a disjoint union of complete graphs. Since G is transtive, every vertex has the same degree. Therefore the graph is a disjoint union of complete graphs of the same size. Since p is prime, this size is either 1 or p. It cannot be 1 as G contains a transposition. Therefore our graph is the complete graph on p vertices, which implies $G = S_p$. □

Example 17.2. *The Galois group of $f(x) = x^5 - 6x + 3$ over $\mathbb{Q}$ is S_5.*

Proof. f is irreducible by Eisenstein's criterion at the prime 3. f has three real roots so complex conjugation gives the existence of a transposition in the Galois group. By Lemma 17.1, the Galois group is S_5. □

Example 17.3. *Let p be a prime and n an integer which is not a p-th power. The Galois group of $f(x) = x^p - n$ over $\mathbb{Q}$ is the group of matrices of the form $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)$ where $a, b \in \mathbb{F}_p$.*

Proof. Let $\zeta = e^{2\pi i/p}$. The assumption that n is not a p-th power implies that $x^p - n$ is irreducible (e.g. because no proper subset of the roots of $x^p - n$ multiply to an integer, as can be seen simply by considering their absolute value). The splitting field contains $\mathbb{Q}[n^{1/p}]$ which is of degree p and $\mathbb{Q}[\zeta]$, which is of degree $p - 1$. Hence $p(p - 1)$ divides the degree of the splitting field. Since the splitting field is contained in $\mathbb{Q}[n^{1/p}, \zeta]$, it is equal to this and of degree $p(p - 1)$.

For every $\alpha \in \mathbb{F}_p^\times$ and $b \in \mathbb{F}_p$, there is a corresponding isomorphism $\sigma_{a,b}$ of $\mathbb{Q}[n^{1/p}, \zeta]$ where

$$\sigma_{a,b}(n^{1/p}) = \zeta^b n^{1/p}, \qquad \sigma_{a,b}(\zeta) = \zeta^a.$$

This is because every automorphism of $\mathbb{Q}[n^{1/p}, \zeta]$ must be of this form, and there are $p(p-1)$ automorphisms of $\mathbb{Q}[n^{1/p}, \zeta]$, hence each of these candidate automorphisms are actually automorphisms. We leave it as an exercise to check the isomorphism with the group claimed in the statement.

□

18. The complex numbers are algebraically closed

There are many proofs that $\mathbb{C}$ is algebraically closed. We give one closest in spirit to the techniques developed in this course.

Theorem 18.1. *The complex numbers are an algebraically closed field.*

Proof. Let K be a finite extension of $\mathbb{R}$. It suffices to show that $K = \mathbb{C}$ or $K = \mathbb{R}$.

Without loss of generality, assume K is Galois over $\mathbb{R}$. Let $G = \mathrm{Gal}(K/\mathbb{R})$. Let P be a Sylow-2-subgroup of G. Let $E = K^P$. Then $[E : \mathbb{R}]$ is odd. By the intermediate value theorem, every odd degree polynomial with coefficients in $\mathbb{R}$ has a real root, hence cannot be irreducible. Therefore $E = \mathbb{R}$ and G is a 2-group.

If $G = \{1\}$ then $K = \mathbb{R}$. Suppose $G \neq 1$. Then as it is a 2-group, it has an index two subgroup H. Let $E = K^H$. Then $[E : \mathbb{R}] = 2$. Since every quadratic polynomial with coefficients in $\mathbb{R}$ has roots in $\mathbb{C}$ by the quadratic formula, it must be that $E = \mathbb{C}$. Now if $H = \{1\}$ then $K = \mathbb{C}$ and we're done. If $H \neq 1$, it has an index two subgroup Q. Let $E = K^Q$. Then $[E : \mathbb{C}] = 2$. But by the quadratic formula, since every complex number has a square root in $\mathbb{C}$, every quadratic polynomial with coefficients in $\mathbb{C}$ has a root in $\mathbb{C}$. Thus there are no quadratic extensions of $\mathbb{C}$, a contradiction. □

19. Solvable Numbers

This section discusses which numbers have expressions involving surds. First a proposition.

Proposition 19.1. *Let $E_0 \subset E_1 \subset E_2 \subset \cdots \subset E_n$ be a tower of fields, with each E_i/E_{i-1} Galois with abelian Galois group. Let K/E_0 be a Galois extension with $K \subset E_n$. Then* $\mathrm{Gal}(K/E_0)$ *is a solvable group.*

Proof. We induct on n, the base case $n = 0$ being trivial. Let L be the smallest subfield of E_n containing K and L (L is the *compositium* of E_1 and K (inside E_n)). If $f \in E_0[x]$ is a polynomial such that E_1 is the splitting field of f and $g \in E_0[x]$ is a polynomial such that K is the splitting field of g, then L is the splitting field of fg. Then L is a Galois extension of E_0 as it is a splitting field.

By induction, $\mathrm{Gal}(L/E_1)$ is solvable. Since $\mathrm{Gal}(L/E_0)/\mathrm{Gal}(L/E_1) \cong \mathrm{Gal}(E_1/E_0)$ which is abelian, this implies that $\mathrm{Gal}(L/E_0)$ is solvable. Since $\mathrm{Gal}(K/E_0)$ is a quotient of $\mathrm{Gal}(L/E_0)$, we conclude that $\mathrm{Gal}(K/E_0)$ is solvable. □

Definition 19.2. *Let $\alpha \in \mathbb{C}$. We say α is solvable if it can be obtained from $\mathbb{Q}$ using a finite number of operations from addition, subtraction, multiplication, division and extracting n-th roots.*

It is clear that every solvable number is algebraic.

Theorem 19.3. *Let $\alpha \in \overline{\mathbb{Q}}$. Let K be the Galois closure of $\mathbb{Q}[\alpha]$. Then α is solvable if and only if* $\mathrm{Gal}(K/\mathbb{Q})$ *is a solvable group.*

We will only discuss the direction where if α is solvable then $\mathrm{Gal}(K/\mathbb{Q})$ is a solvable group. The other direction requires Kummer theory.

Proof. (Sketch): Inductively construct a tower of fields $\mathbb{Q} = E_0 \subset E_1 \subset E_2 \subset \cdots$. First take $E_1 = \mathbb{Q}[e^{2\pi i/n}]$ for some n. Then for $k \geq 1$, make each E_{k+1}/E_k to be adjoining a d-th root of some element in E_k, for some $d \mid n$. If α is solvable, every Galois conjugate of α is also solvable, then the tower can be extended so that every Galois conjugate of α lies in E_N for some N. Then K is a subfield of E_N.

Show that each extension E_{k+1}/E_k is Galois with abelian Galois group.

The situation is now as follows: We have K/E_0 Galois with Galois group G. We have a tower of field extensions $E_0 \subset E_1 \subset \cdots \subset E_N$ with each E_{k+1}/E_k Galois with abelian Galois group. The solvability of $\mathrm{Gal}(K/\mathbb{Q})$ follows from Proposition 19.1. □

20. Finite fields

Theorem 20.1. *Let q be a power of a prime p. Then there exists a unique field with q elements.*

Proof. First we show existence. Let F be the splitting field of $f(x) = x^q - x$ over $\mathbb{F}_p$. Note that as $f'(x) = -1$, $f(x)$ has no multiple roots in F, hence has exactly q roots in F. Let

$$F' = \{y \in F \mid y^q = y\}.$$

Then $|F'| = q$ and by Freshman's Dream[2], F' is a subfield of F. This concludes existence.

Now let K be a field of order q. Since q is a power of p, K is a finite extension of $\mathbb{F}_p$. By the primitive element theorem we can find $g(x) \in \mathbb{F}_p[x]$ such that $K \cong F[x]/(g(x))$. Since $g(x)$ divides $x^q - x$, $g(x)$ has a root in F'. Let α be this root. Then $x \mapsto \alpha$ defines an injection of fields from K to F'. Since they have the same cardinality, they are the same, proving uniqueness. □

Remark 20.2. In the above proof, the field F' is actually equal to F.

The unique field of order q is often denoted $\mathbb{F}_q$.

[2] Freshman's Dream is the identity $(x+y)^q = x^q + y^q$

21. Cyclotomic Polynomials

(This section is unlikely to be explicitly covered in the course). Let n be a positive integer. The n-th cyclotomic polynomial $\Phi_n(x) \in \mathbb{Z}[x]$ is defined to be

$$\Phi_n(x) = \prod_{\substack{1 \leq k \leq n \\ \gcd(k,n)=1}} (x - e^{\frac{2\pi i k}{n}}).$$

An alternative description is

$$\prod_{d|n} \Phi_d(x) = x^n - 1,$$

which makes it clear that $\Phi_n(x) \in \mathbb{Z}[x]$ by induction on n.

Theorem 21.1. *For all integers n, the polynomial $\Phi_n(x)$ is irreducible.*

Remark 21.2. When n is a power of a prime, we can prove this using Eisenstein's criterion. The prove we give here does not specialise to that proof.

Proof. Suppose $\Phi_n(x) = g(x)h(x)$ for some $g(x), h(x) \in \mathbb{Z}[x]$. Let p be a prime that does not divide n. Let ζ be a root of $g(x)$. We will show that ζ^p is a root of $g(x)$.

Suppose not, then ζ^p is a root of $h(x)$, so ζ is a root of $h(x^p)$. Therefore $h(x^p)$ and $g(x)$ have a common factor. Reducing modulo p, we see that $h(x^p) = h(x)^p$ and $g(x)$ have a common factor modulo p, i.e. $h(x)$ and $g(x)$ have a common factor modulo p. But then $x^n - 1$ has a double root modulo p, which is not true as its derivative is nx^{n-1}, which only has the root zero, as $p \nmid n$.

We have shown that if ζ is a root of $g(x)$, then ζ^p is also a root of $g(x)$. Since this is true for all primes p coprime to n, either $g(x)$ is constant or all primitive n-th roots of 1 must be roots of $g(x)$, which means $h(x)$ is constant. Therefore $\Phi_n(x)$ is irreducible. □

We can now prove the following generalisation of Example 14.5:

Theorem 21.3. *The field $\mathbb{Q}[e^{\frac{2\pi i}{n}}]$ is a Galois extension of $\mathbb{Q}$ with Galois group $(\mathbb{Z}/n\mathbb{Z})^\times$*

22. Trancendental Numbers

This is an optional extra. The set of polynomials with coefficients in $\mathbb{Q}$ is countable, hence the set of complex numbers algebraic over $\mathbb{Q}$ is countable. So, in one very precise measure-theoretic sense, almost all complex numbers are trancendental.

The simplest way to write down a trancendental number is to take a limit of a sequence that converges too fast. For example

$$\sum_{n=1}^{\infty} \frac{1}{2^{f(n)}}$$

works as long as $f : \mathbb{N} \to \mathbb{N}$ grows fast enough. It is not hard to show that if α is algebraic and irrational, then there exists d and C such that

$$\left| \alpha - \frac{p}{q} \right| > Cq^{-d}$$

for all integers p, q with $q \neq 0$. With this criteria, we can easily create trancendental numbers of the type mentioned above.

To actually prove that certain numbers we care about are trancendental is another story.

Theorem 22.1. *e is trancendental.*

Proof. First the rabbit. The introduction of this function is the part of this proof I don't know how to motivate. Let f be a polynomial and define

$$I(z, f) = \int_0^z e^{z-t} f(t)\, dt.$$

Integrating by parts gives the recursion

$$I(z, f) = e^z f(0) - f(z) + I(z, f')$$

from which we get the formula

$$I(z, f) = e^z \sum_{j \geq 0} f^{(j)}(0) - \sum_{j \geq 0} f^{(j)}(z).$$

Now suppose that there exist integers $a_0, a_1, \ldots, a_d$, not all zero, such that $\sum_{n=1}^d a_n e^n = 0$. Without loss of generality suppose that $a_0 \neq 0$. Then

$$\sum_{n=0}^d a_n I(n, f) = \sum_{n=0}^d a_n \sum_{j \geq 0} f^{(j)}(n).$$

Let $f(x) = x^{p-1} \prod_{n=1}^d (x-i)^p$ where p is a prime to be determined later. From the standard bound on an integral being at most the length of the interval times the maximum absolute value of the integrand, we obtain a bound of the form

$$\left| \sum_{n=0}^d a_n I(n, f) \right| \leq AB^p$$

for some real numbers A and B.

Since f has integer coefficients, $f^{(j)}(n)$ is divisible by $j!$ for all j and all integer n. Also $f^{(j)}(n) = 0$ if $n \in \{0, 1, 2, \ldots, d\}$ and $j < p$, except for $n = 0$ and $j = p - 1$, since in each case f has a zero of multiplicity at least $j + 1$. Therefore

$$\sum_{n=0}^d a_n \sum_{j \geq 0} f^{(j)}(n) \equiv a_0 f^{(p-1)}(0) \pmod{p!}.$$

If $p > d$ and $p \nmid a_0$, then $a_0 f^{(p-1)}(0)$ is not divisible by p, so in particular is nonzero. The number is divisible by $(p-1)!$, which implies

$$\left| \sum_{n=0}^d a_n \sum_{j \geq 0} f^{(j)}(n) \right| \geq (p-1)!.$$

Since there are infinitely many primes, we may choose a prime p such that $AB^p < (p-1)!$ to get a contradiction. □

Remark 22.2. It is possible to use the same rabbit to give a proof that π is trancendental. A writeup is at http://www.petermc.net/blog/2017/02/04/pi-is-trancendental/

Email address: maths@petermc.net