Introduction to Rings & Fields

Lecture Notes
by
Stefan Waner

(second printing: 2003)

Department of Mathematics, Hofstra University

Rings and Fields

1. Rings, Subrings and Homomorphisms

The axioms of a ring are based on the structure in Z.

Definition 1.1 A **ring** is a triple $(R, +, \cdot)$ where R is a set, and + and · are binary operations on R (called **addition** and **multiplication** respectively) so that:

(1) $(R,+)$ is an abelian group (with identity denoted by 0 and the inverse of $x \in R$ denoted by $-x$, as usual.)

(2) Multiplication is associative.

(3) The following distributive laws hold $\forall x, y, z \in R$:

$x(y+z) = xy + xz$ (left distributive law)

$(x+y)z = xz + yz$ (right distributive law)

Notes

(1) Multiplication need not be commutative. If it is, R is called a **commutative ring**.

(2) There need not be a multiplicative identity nor multiplicative inverses.

Examples 1.2

(A) $R = \{0\}$, the trivial ring.

(B) Z, Q, R and C.

(C) $M(n;\mathrm{A})$, the ring of $n \times n$ matrices with entries in A = Z, Q, R or C.

(D) Z/nZ, under the operations $[x]+[y] = [x+y]$; $[x][y] = [xy]$. (We showed they were well-defined in Math 145.)

(E) $n\mathrm{Z} \subset \mathrm{Z}$

(F) Map(R,R), the set of maps R⟶R.

(G) Z[i], the ring of **Gaussian Integers**, given by

$\mathrm{Z}[i] = \{a + ib \in \mathrm{C} \mid a, b \in \mathrm{Z}\}$.

(H) Z×Z, under pointwise addition and multiplication.

(I) More generally, if R and S are rings, then $R \times S$ inherits the structure of a ring.

Important Examples 1.3

Let R be any ring. The **associated polynomial ring** $R[x]$ is defined as follows: The elements of $R[x]$ are all formal expressions of the form

$$a_0 + a_1x + a_2x^2 + \ldots + a_nx^n + \ldots = \sum_{i=0}^{\infty} a_ix^i$$

where $a_i \in R$, $a_i = 0$ for $i \geq$ some n, and x is just a meaningless symbol. Examples of elements of Z[x] are $1 + x$, $1 - x^2 + x^4$, $2x$, 0 and $11x^{99} + x^{1,000}$.

Addition and multiplication are is defined in the expected way:

$$(a_0 + a_1x + a_2x^2 + \ldots) + (b_0 + b_1x + b_2x^2 + ..)$$
$$= (a_0+b_0) + (a_1+b_1)x + (a_2+b_2)x^2 + ..$$

and multiplication by

$$(a_0 + a_1x + a_2x^2 + \ldots)(b_0 + b_1x + b_2x^2 + ..)$$
$$= a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \ldots$$

Formally,

$$\sum_{i=0}^{\infty} a_ix^i + \sum_{i=0}^{\infty} b_ix^i = \sum_{i=0}^{\infty}(a_i+b_I)x^i$$
$$\left(\sum_{i=0}^{\infty} a_ix^i\right)\left(\sum_{i=0}^{\infty} b_ix^i\right) = \sum_{i=0}^{\infty}\left(\sum_{j+k=i}(a_jb_k)\right)x_i.$$

If we lift the restriction that all but finitely many of the a_i are zero, we get the **ring of power series** $R[[x]]$, with addition and multiplication defined in the same way.

Note that $R[x] \subset R[[x]]$.

Lemma 1.4
If R is a ring, then $\forall a, b \in R$, we have
(a) $0.a = a.0 = 0$ for all $a \in R$;
(b) $a(-b) = (-a)b = -ab$;
(c) $(-a)(-b) = ab$.

Definition 1.5 A **ring with 1** is a ring with a multiplicative unit (denoted by 1). Thus, for all $a \in R$, $a.1 = 1.a = a$. We refer to a commutative ring with 1 as a crw1.

Examples Look at those above to pick out the crw1's.

Definition 1.6 A **subring** of the ring R is a subset S such that:
(1) S is a subgroup of R under addition;
(2) S is closed under multiplication

Lemma 1.7
A subring of a ring R inherits the structure of a ring from R.

Examples 1.8
(A) $n\mathrm{Z} \subset \mathrm{Z}$ **(B)** $\mathrm{Z}\times\{0\} \subset \mathrm{Z}\times\mathrm{Z}$
(C) $R[x] \subset R[[x]]$ **(D)** Various others in class

Definition 1.9 Let R and R' be rings. A **ring homomorphism** is a map f: $R \longrightarrow R'$ such that:

(1) $f(a+b) = f(a)+f(b)$
(2) $f(ab) = f(a)f(b)$

$\forall a,\ b \in$ R. As in group theory, we also have **endomorphisms** (homs $R\longrightarrow R$), **monomorphisms, epimorphisms, isomorphisms and automorphisms**. These are defined in the usual way.

Notes

(1) Property (1) says that f is a group homomorphism
(2) If R has 1, then $f(1_R)$ *need not be* $1_{R'}$, as Example (C) below will show.

Examples 1.10

(A) f: Z$\longrightarrow$Z; $f(x) = -x$ is *not* a ring homomorphism (why)
(B) f: Z$\longrightarrow$Z/nZ; $f(x) = [x]$
(C) f: Z$\longrightarrow$Z×Z; $f(n) = (n,0)$ (D) π: $R\times S\longrightarrow R$.
(E) The **augmentation map** ε: $R[x]\longrightarrow R$
(F) The **evaluation maps** f_a: $R[x]\longrightarrow R$ for $a \in R$.

Exercise Set 1

From Herstein p. 130:
(a) If R is a ring and $a, b, c, d \in R$, evaluate $(a + b)(c + d)$
(b) Prove that, if $a, b \in R$, then $(a + b)^2 = a^2 + ab + ba + b^2$, where by x^2 we mean xx.
(c) Find the form of the binomial theorem in a general ring; in other words, find an expression for $(a + b)^n$, where n is a positive integer.
Prove that $R[x]$ and $R[[x]]$ satisfy the axioms of a ring.
Define Z[$\sqrt{2}$] as $\{a + b\sqrt{2} \mid a, b \in$ Z$\}$. Show that Z[$\sqrt{2}$] is a crw1.

Hand In:

1. Prove that, if R is a crw1 such that $0 = 1$, then $R = \{0\}$.
2. Prove that there are only two ring endomorphisms of Z.
3. Prove that, if the ring R has a 1, then it is unique.
4. Prove that, if f: $R\longrightarrow R'$ is a ring homomorphism, then:
(a) $f(R)$ is a subring of R'
(b) $\ker f = f^{-1}(0)$ is a subring of R
(c) if R has 1 and f: $R\longrightarrow R'$ is a ring epimorphism, then $f(1_R) = 1_{R'}$.
5. Give examples of the following:
(a) A ring monomorphism f: $M(2;$R$)\longrightarrow M(3;$R$)$
(b) A ring automorphism of Z[x] other than the identity
6. Is the derivative map D: R[x]$\longrightarrow$R[x] given by $D(p(x)) = p'(x)$ a ring homom-orphism? Justify your claim.
7. Show that, in Z/pZ (p prime) one has $(x + y)^p = x^p + y^p$. (See your Math 145 Exercises.)
8. (Herstein p. 130 # 9) Prove that commutativity of addition in a ring R with 1 follows from the other axioms. (Hint: Expand $(a+b)(1+1)$ in two ways, using left- and right-distributivity.)

9. (Herstein p. 130 # 4) Prove that, if a ring R has the property that $x^2 = x$ for every $x \in R$, then R is commutative. (Warning: you can not assume the cancellation law for multiplication!)

2. Units, Zero Divisors and Integral Domains

In this section, R will denote a ring with 1. Also, from now on we assume $1 \neq 0$ (or else our ring will be $\{0\}$, as we have seen).

Definition 2.1 An element $u \in R$ is called a **unit** if it has a multiplicative inverse; that is, there exists $u' \in R$ such that $uu' = u'u = 1$.

Examples 2.2

(A) Units in Z　　**(B)** Units in Z×Z
(C) Units in R×R　　**(D)** Units in Z/nZ
(D) Units in Z/pZ; p prime

Note
If u is a unit, then its multiplicative inverse is unique.

Definition 2.3 Let R be a crw1. Then a **zero divisor** is an element $s \in R$ such that $s \neq 0$ and there exists an element $r \in R$ with $r \neq 0$ and $rs = 0$.

Examples 2.4

(A) Z×Z has many of them　　**(B)** $M(n,$R$)$ too
(C) Z, Q, R, C have none　　**(D)** Z[x] has none
(E) Z/6Z has three: [2], [3] and[4].

Before going on to settle the case for Z/nZ, we need a little number theory about common factors, etc.

Definition 2.5 If R is any commutative ring and $r, s \in R$, we say that r **divides** s, and write $r|s$ if there exists $k \in R$ such that $s = kr$.

Proposition 2.6 (Zero Divisors in Z/*n*Z)
Let $1 \leq m \leq n-1$. Then $[m] \in$ Z/nZ is a zero divisor iff $(m, n) \neq 1$.

Proof

$\boxed{\Rightarrow}$ If $[m]$ is a zero divisor then $[m] \neq 0$ and there is a k with $[k] \neq 0$ and $[m][k] = 0$. If $(m,n) = 1$, then there would exist integers r and s with

$$rm + sn = 1$$

giving $[r][m] = [1]$
Multiplying by k:

$$[r][m][k] = [1][k] = [k]$$

But the left-hand side is zero because $[m][k] = 0$,
so that $[k] = 0$,
a contradiction.

$\boxed{\Leftarrow}$ Assume that $(m,n) \neq 1$. Then m and n have a common factor $h > 1$. Write $m = ha$ and $n = hb$, with $0 < b < n$ (since $h \neq 1$ implies $b \neq n$.) Then

$$[m][b] = [hab] = [an] = [0],$$

even though the inequality above shows that $[b] \neq [0]$.

Corollary 2.7 If p is prime, then Z/pZ has no zero divisors.

Definition 2.8 An **integral domain** is a crw1 D such that D contains no zero divisors.

Examples 2.9

(A) Z, Q, R, C **(B)** A[x], where A = Z, Q, R or C

(C) Z/nZ, iff p is prime **(D)** Z×Z and $M(n,$A) are *not* domains.

Lemma 2.10 (You can cancel in Integral Domains)
If D is an integral domain, then the cancellation law holds; viz.

$$ax = ay \Rightarrow x = y$$

Exercise Set 2

Notation: Henceforth, we write Z/nZ as Z_n.

1. Show that the set of units in a ring with 1 form a group under multiplication, and illustrate this by identifying the group of units in $M(n;$R).

2. Prove that, if R is a crw1 that is *not* an integral domain, then the cancellation law fails; that is, there exist elements a, x and y with $ax = ay$, but $x \neq y$.

3. **(a)** An element $e \in R$ is an **idempotent** if $e^2 = e$. Prove that, if D is a domain, then it has exactly two idempotent elements: 1 and 0.

(b) Find two idempotent elements other than the identity and zero ("nontrivial idempotents") in each of Z×Z and $M(n,$Z), and find one in Z_6.

(c) Find six nontrivial idempotents in Z×Z×Z.

(d) Show that, if e is an idempotent in the commutative ring R, then

(i) $1-e$ is also an idempotent

(ii) $2e-1$ is a unit [Hint: multiply it by various things…]

4. Show that, if R is a ring with 1 and f: $R \longrightarrow D$ is any non-zero ring homomorphism with D an integral domain, then $f(1_R) = 1_D$.

5. Prove that Z_n is an integral domain iff n is prime.

3. Fields

Definition 3.1 A **field** K is an integral domain in which every non-zero element is a unit.

Examples 3.2

(A) Q, R and C **(B)** Z/pZ (p prime) ?? (See below.)

(C) Z and R[x] are *not* fields, even though they are integral domains.

(D) Q[$\sqrt{2}$] = $\{r + s\sqrt{2} \mid r, s \in$ Q$\}$.

Proposition 3.3 (Finite Integral Domains)
Every finite integral domain is a field.

Proof. Let $D = \{0, 1, d_1, d_2, \dots, d_n\}$ be a finite integral domain, and let d be any of its non-zero elements. Then the elements $d.0, d.1, d.d_1, d.d_2, \dots, d.d_n$ must all be distinct, by the cancellation law. Thus $\{d.0, d.1, d.d_1, d.d_2, \dots, d.d_n\}$, having the same number of elements as D, must be equal to D, and hence must contain 1. In other words, $dx = 1$ for some $x \in D$. ❒

Corollary 3.4 Z/pZ is a field iff p is prime.

Lemma 3.5 If K is a field, then the non-zero elements of K form a group under multiplication.

The following construction shows that every domain can be enlarged to a field.

Construction 3.6 (The Field of Fractions of an Integral Domain)
Let D be an integral domain, and define an equivalence relation on $D\times(D-\{0\})$ by

$$(a, b) \approx (c, d) \text{ iff } ad = bc.$$

(You will check in the homework that it is indeed an equivalence relation. Let K be the set of equivalence classes. Now define addition and multiplication on K by:

$$[(a, b)] + [(c, d)] = [(ad+bc, bd)]$$
$$[(a, b)][(c, d)] = [(ac, bd)]$$

(You will check that they are well-defined in the homework.) Further, these operations turn K into a field, called the **field of fractions** of D. (We check some of the properties in class and assign others as exercises.) Further, the map ι: $D \longrightarrow K$ given by $\iota(a) = [(a, 1)]$ is a ring monomorphism, showing that ι is a ring isomorphism onto its image. In other words, D is isomorphic to a subring of its field of fractions K. Note that the field of fractions of Z is just Q. The map ι: Z$\longrightarrow$Q is just the map $\iota(n) = [(n, 1)]$ (or ${}^{n}/_{1}$). This map allows us to think of integers as rational numbers, and we regard Z as a subring of Q via this map. Thus we now know how to construct the rationals with our bare hands.

Note
In the exercises, we shall see that K is the smallest field containing D. Thus, when, for example, you are looking for the field of fractions of a subring of R, look for the smallest subfield of R containing it.

Exercise Set 3
1. Prove that Q[$\sqrt{2}$, $\sqrt{3}$] = $\{r + s\sqrt{2} + t\sqrt{3} + u\sqrt{6} \mid r, s, t, u \in$ Q$\}$ is a field.
2. What are the smallest subfields of R containing Z[i] and Z[$\sqrt{2}$]? [Hint: You will finally discover why you were told over and over again to "rationalize the denominator!" when you were very little (even though your kindergarten math teacher probably didn't have a clue as to the reason why! My high school teacher told me that π was 22/7. We shall learn (but unfortunately not prove) later in the course that it is not only irrational, but "transcendental."))]

3. **(a)** Prove that the relation on $D \times (D - \{0\})$ given by $(a, b) \approx (c, d)$ iff $ad = bc$ is an equivalence relation.

(b) Prove that addition and multiplication as defined in Construction 4.4 are well defined.

(c) Prove that addition in K is associative.

4. Show that every field is isomorphic to its own field of quotients.

5. Fermat's Little Theorem

(a) Let p be prime, and let $[n] \in \mathrm{Z}/p\mathrm{Z}$ be any non-zero element. Recalling that the set of non-zero elements in a field form a multiplicative group, and recalling Lagrange's theorem, show that $[n]^{p-1} = [1]$. Deduce **Fermat's Little Theorem:** If n is any integer not divisible by the prime p, then $n^{p-1} \equiv 1 \bmod p$.

(b) Deduce that, if n is any integer not divisible by the prime p, then $n^p \equiv n \bmod p$.

6. Prove that, if f: $K \longrightarrow L$ is a non-zero field homomorphism (that is, a non-zero ring homomorphism from one field to another) then:

(i) $f(1_K) = 1_L$

(ii) $f(k^{-1}) = f(k)^{-1}\ \forall k \in K$.

7. Universal Property of the Field of Fractions Let D be a domain, and let K be its field of fractions.

(a) Prove that, if f: $D \longrightarrow L$ is any ring monomorphism from D into a field L, then there exists a unique ring monomorphism g: $K \longrightarrow L$ such that the diagram

$$\begin{tikzcd} D \arrow[r, "f"] \arrow[d, "\iota"'] & L \\ K \arrow[ur, "g"'] & \end{tikzcd}$$

commutes. (Roughly speaking, any field containing a copy of D as a subring must necessarily contain a copy of K also, so K is the *smallest field containing* D.)

(b) Let D be a domain. We say that a field K (not necessarily the field of fractions of D) has the **universal property for a field of fractions of** D if there exists a monomorphism ι: $D \longrightarrow K$ with the property described in (a), viz: if f: $D \longrightarrow L$ is any ring monomorphism from D into a field L, then there exists a unique ring monomorphism g: $K \longrightarrow L$ such that the diagram

$$\begin{tikzcd} D \arrow[r, "f"] \arrow[d, "\iota"'] & L \\ K \arrow[ur, "g"'] & \end{tikzcd}$$

commutes. Show that, if K and K' both have the universal property for a field of fractions of D, then K and K' are isomorphic. (Roughly speaking, the field of fractions is unique, given its universal property.)

8* The ring of real **Laurent Series** L$[x]$ is the ring of all series of the form $\sum_{i=-\infty}^{\text{Ï}} a_i x^i$, where $a_i \in \mathrm{R}$, $a_i = 0$ for $i \leq$ some n (possibly negative). Thus typical elements are $x + x^2 + x^3 + \ldots$, $\frac{1}{x^2} - \frac{1}{x} + 2x^{765}$. (The series all start somewhere, but need never end). Show that L$[x]$ is in fact the field of fractions of $\mathrm{R}[[x]]$ but not $\mathrm{R}[x]$. [Hint: to find the inverse of a polynomial, try the brute force approach of dividing it into 1!]

4. The Ring of Polynomials over a Field

Let K be a field, and recall the definition of $K[x]$. Note also that we have an evaluation homomorphism of rings ε_a: $K[x] \longrightarrow K$ given by $\varepsilon_a(p(x)) = p(a)$ for every $a \in K$.

Definition 4.1 The **degree** of the polynomial $p(x) = a_0 + a_1x + \ldots + a_nx^n + \ldots$ in $K[x]$ is the largest power of x with a non-zero coefficient. We denote the degree of $p(x)$ by $\delta(p(x))$. We also define $\delta(0) = -\infty$.

Lemma 4.2 (Degree of a Product)
If $p(x)$ and $q(x) \in K[x]$, then:

$$\delta(p(x)q(x)) = \delta(p(x)) + \delta(q(x)).$$

Proof in the exercise set.

Corollary 4.3 $K[x]$ is an integral domain.

Note: All the above also works with K replaced by any integral domain, such as Z.

The following theorem is fundamental.

Theorem 4.4 (Euclid's Division Algorithm)
Let $f(x)$ and $g(x) \in K[x]$ be such that $g(x) \neq 0$, $\delta(g(x)) \leq \delta(f(x))$. Then there exist unique polynomials $q(x)$ and $r(x)$ such that

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

with $\delta(r(x)) < \delta(g(x))$

Proof We first show existence, by induction on $n = \delta(f(x)) - \delta(g(x))$. If $n = 0$, then $f(x)$ and $g(x)$ have the same degree m, so write

$$f(x) = a_0 + a_1x + \ldots + a_mx^m \ (a_m \neq 0)$$

and $$g(x) = b_0 + b_1x + \ldots + b_mx^m \ (b_m \neq 0).$$

Then we have

$$f(x) = g(x)\frac{a_m}{b_m} + \left(f(x) - g(x)\frac{a_m}{b_m}\right),$$

where the second term has degree $< m = \delta(g(x))$, showing the case for $n = 0$. Now for the inductive step. Assume the result true for $k \leq n-1$, and that $\delta(f(x)) - \delta(g(x)) = n$. Then, for some m,

$$f(x) = a_0 + a_1x + \ldots + a_mx^m + \ldots + a_{m+n}x^{m+n} \ (a_{m+n} \neq 0)$$

and $$g(x) = b_0 + b_1x + \ldots + b_mx^m \ (b_m \neq 0).$$

Write:

$$f(x) = g(x)x^n\frac{a_{m+n}}{b_m} + \left(f(x) - g(x)x^n\frac{a_{m+n}}{b_m}\right) = g(x)x^n\frac{a_{m+n}}{b_m} + k(x),$$

say. Now $k(x)$ has degree $\leq m+n-1$. If its degree is $< \delta(g(x))$, we take $r(x) = k(x)$, and are done. If not by the inductive hypothesis applied to the pair $(k(x), g(x))$, we can write

$$k(x) = g(x)t(x) + r(x),$$

where $\delta(r(x)) < \delta(g(x))$. Substituting for $k(x)$ in the above equation gives:

$$f(x) = g(x)x^n\frac{a_{m+n}}{b_m} + g(x)t(x) + r(x) = g(x)\left(x^n\frac{a_{m+n}}{b_m} + t(x)\right) + r(x).$$

Done.

Uniqueness: S'pose we can write:

$$f(x) = g(x)q(x) + r(x) = g(x)q^*(x) + r^*(x)$$

as per the theorem. Then subtracting gives:

$$g(x)[q(x)-q^*(x)] + [r(x)-r^*(x)] = 0,$$

or $\quad g(x)[q(x)-q^*(x)] = -[r(x)-r^*(x)]$.

If $q(x)-q^*(x) \neq 0$, then it has degree at least 0, so the degree on the left is at least that of $g(x)$ (by Lemma 5.1) while the degree on the right is < that of $g(x)$, a contradiction. Thus $q(x) = q^*(x)$, whence also $r(x) = r^*(x)$. ❒

Corollary 4.5 (**Remainder Theorem**)
S'pose $p(x) \in K[x]$ has degree ≥ 1 and $a \in K$. Then $p(a)$ is the remainder when $p(x)$ is divided by $(x-a)$. Thus, if $p(a) = 0$, then $(x-a)$ is a factor of $p(x)$.

Proof. Dividing $p(x)$ by $(x-a)$ gives

$$p(x) = (x-a)q(x) + r,$$

where we have written the remainder as an element of K, since its degree is < 1. Evaluating everything at a gives the result. ❒

Definition A **zero** of the polynomial $p(x) \in K[x]$ is an element $a \in K$ such that $p(a) = 0$.

Corollary 4.6 If $\delta(p(x)) = n$, then $p(x)$ can have at most n distinct zeros.

Proof. We do induction on n. The result certainly holds if n=0. Thus assume the result is true for all polynomials of degree ≤ $n-1$, and let $p(x)$ have degree n. Then let a be any zero of $p(x)$. Since $p(a) = 0$, the remainder theorem says that $(x-a)$ is a factor of $p(x)$, and so

$$p(x) = (x-a)q(x),$$

with $\delta(q(x)) = n-1$ (by Lemma 5.1) Claim: all other zeros of $p(x)$ are also zeros of $q(x)$. Indeed, if b is one such, then $0 = p(b) = (b-a)q(b)$, so that, since $(b-a) \neq 0$ and K has no zero divisors, it must be the case that $q(b) = 0$. Since $q(x)$ has degree $n-1$, it can have at most $n-1$ zeros, by the induction hypothesis, so we are done, since this means that $p(x)$ can have at most $n-1$ more zeros. ❒

Note Euclid's Theorem fails if K is not a field. For instance, in Z[x], we cannot divide x^2+1 by $2x$ and get a quotient and remainder as in the theorem. However, as we shall see, the remainder theorem still works.

Definition 4.7 $p(x) \in K[x]$ is **irreducible over** $\boldsymbol{K}$ if has degree ≥ 1 and cannot be expressed as a product of polynomials of lower degree.

Examples 4.8

(A) x^2-2 is irreducible over Q but not over R.
(B) x^2+1 is irreducible over R but not over C.
(C) $x^3+ 3x+2$ is irreducible over Z_5, but not over R.

(D) Let p be prime. Then the **cyclotomic** polynomial,

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1$$

is irreducible over Z. (See Fraleigh, p. 327.)

Exercise Set 4

1. Prove Lemma 4.2

2. Use the remainder theorem to completely factor x^4+4 in $Z_5[x]$.

3. Show that $x^3 + 2x + 4$ is irreducible in $Z_5[x]$.

4. Find all irreducible polynomials of degree 3 in $Z_3[x]$.

5 (a) Show that if $p(x) \in Z_2[x]$ then either $p(x)$ is divisible by $x+1$, or else $p(x)+1$ is.

(b) Generalize this to a result about $Z_n[x]$.

5. A Result on Factorization of Polynomials over Q

We want to be honest[†] in our proof that you can't trisect angles and do other kinds of ruler-and-compass constructions, and it will turn out that, to do this, we shall need to show that certain polynomials are irreducible over Q. To do *that*, we shall appeal to the following theorem.

Theorem 5.1 (Irreducibility over Q)
Let $p(x)$ be any polynomial with coefficients in Z. Then $p(x)$ is irreducible in $Q[x]$ iff it is irreducible in $Z[x]$.

Before going to the proof, let us contemplate the majestic power of this result:

Examples 5.2

(A) $x^3 - 3x - 1$ is irreducible over Q, since if it were not, it would factor over the integers as well (by the theorem). But then it would have a linear factor which must be of the form $(x \pm 1)$ (looking at the coefficients of x^3 and 1). But putting $x = \pm 1$ does not give zero, so it can't be a factor.

(B) $x^4 - 2x^2 + 8x + 1$ is also irreducible over Q. Indeed, if it were not, then it would also factor over Z. But it can't have any linear factors over Z for the same reason as Example (A). Thus, if it does factor over Z, it must have two quadratic factors as follows

$$x^4 - 2x^2 + 8x + 1 = (x^2 + ax \pm 1)(x^2 + bx \pm 1)$$

where, looking at the coefficients of x and x^3, we must have $a + b = \pm 8$, $a + b = 0$, a contradiction.

(C) $8x^3 - 6x - 1$ is also irreducible over Q, since the only possible linear factors over Z are: $(8x \pm 1)$, $(4x \pm 1)$, $(2x \pm 1)$ or $(x \pm 1)$, and none of them are factors. (We will see that it is a consequence of this that we can't trisect an angle.)

Proof of Theorem

[†] That is, we don't want to appeal to theorems we haven't proved!

□ If $p(x)$ is irreducible in Q[x], then it cannot be written as a product of polynomials of smaller degree with rational coefficients—let alone *integer* coefficients. Thus it is irreducible in Z[x] *a fortiori*.

□ (the harder direction) S'pose $p(x)$ is irreducible in Z[x], and s'pose that it was not irreducible in Q[x]. Thus, as an element of Q[x], we can write

$$p(x) = r(x)s(x)$$

u u u
in Z[x] in Q[x]

where $r(x)$ and $s(x)$ are in Q[x] and have smaller degree than $p(x)$. To obtain a contradiction, we want to convert this into an equation of polynomials in Z[x]. This we do with our bare hands as follows. First, note that we can clear all denominators from the coefficients by multiplying both sides by a large enough integer N. In other words,

$$Np(x) = t(x)u(x)$$

where $t(x)$ and $u(x)$ are now in Z[x] and have the same degrees as $r(x)$ and $s(x)$. Now we are dealing with polynomials over Z.

Next, we prove a little

Lemma 5.3 (Primes numbers act like Prime Polynomials in Z[*x*])
If $u(x)$ and $t(x) \in$ Z[x], and q is any prime in Z such that q divides $t(x)u(x)$ in Z[x], then q $|t(x)$ or $q|u(x)$ (in Z[x]).

Proof: Since q divides $t(x)u(x)$, all of its coefficients must be divisible by q. (Look at what it means for q to divide a polynomial.) Now write

$$t(x) = \Sigma a_i x^i,\ u(x) = \Sigma b_i x^i.$$

S'pose that q divides *neither* $t(x)$ nor $u(x)$. Then there is an a_i and a b_j such that neither are multiples of q. Assume we have chosen such a pair for the largest i and j (so that all the larger coefficients of both, if any, are divisible by p) Then look at the coefficient c_{i+j} of x^{i+j} in $t(x)u(x)$:

$$c_{i+j} = a_i b_j + \text{ sums of terms of the form } a_r b_s \text{ with either } r>i \text{ or } s>j.$$

But, by our choice of i and j, all the terms $a_r b_s$ (if any) are divisible by q. Further, so is c_{i+j}, since it is a coefficient of the product $t(x)u(x)$. Thus, by the 2-out-of-3 rule, $a_i b_j$ is in fact divisible by q. But q is a prime. Thus either a_i or b_j is divisible by q, a contradiction. ❐

Going back to our equation in Z[x]:

$$Np(x) = t(x)u(x),$$

we can now start chopping away at N by dividing both sides by its prime factors using the lemma at each stage: If q is any prime factor of N, then since q divides the LHS, it also divides the RHS, so, by the lemma, it must divide either $t(x)$ or $u(x)$—assume, *wlog*, it divides $t(x)$. Then we can write:

$$qMp(x) = (qw(x))u(x).$$

with everything in Z[x]. Since Z[x] is a domain, we can cancel the q from both sides, obtaining

$$Mp(x) = w(x)u(x).$$

Note that $w(x)$ and $u(x)$ still have the same degrees as our original $r(x)$ and $s(x)$. Now we can keep going inductively until we have reduced M to 1, obtaining

$$p(x) = a(x)b(x)$$

in Z[x], where $a(x)$ and $b(x)$ have smaller degree than $p(x)$. But this contradicts the fact that $p(x)$ was irreducible in Z[x]. ❐

Exercise Set 5

1. Prove that every irreducible in Q[x] has the form $q(x)/n$ for some irreducible $q(x)$ in Z[x] and some integer n. [Hint: show that if $p(x)$ is irreducible in Q[x], then $n{\cdot}p(x)$ is irreducible in Z[x] for some integer n.]

6. Ideals

From now on all rings R will be assumed to be crw1's. (Bye-bye, matrix rings!)

Definition 6.1 An **ideal** in the ring R is an additive subgroup J such that $rj \in J$ for every $r \in R$ and $j \in J$.

Note: An ideal is automatically a subring, and more.

Examples 6.2

(A) The **trivial ideal** $\{0\} \subset R$

(B) nZ ⊂ Z

(C) More generally, if $s \in R$, $Rs = \{rs : r \in R\} = \langle s\rangle$

(D) $K[x] = \langle 1\rangle \supset \langle x\rangle \supset \langle x^2\rangle \supset \dots$ is a **descending chain** of ideals.

(E) The kernel of an ring hom.

(F) The only ideals in a field K are $\{0\}$ and K.

(G) If I and J are ideals, then define $I{+}J = \{i{+}j \mid i \in I \text{ and } j \in J\}$.

Lemma 6.3 If J is an ideal, and $1 \in J$, then $J = R$.

Theorem 6.4 (**Quotient Rings**)
Let $J \lhd R$. Then The set R/J of additive cosets $r+J$ forms a crw1, with

$$(r+J) + (s+J) = (r+s)+J;$$
$$(r+J)(s+J) = rs+J.$$

Examples 6.5

(A) $\mathrm{Z}/n\mathrm{Z}$ (B) $K[x]/\langle x\rangle$

(C) $K[x]/\langle x^2\}$ (D) $K[x,y]/\langle y\rangle$

(E) $(\mathrm{Z}\times\mathrm{Z})/(\mathrm{Z}\times\{0\})$ (F) $\mathrm{Z}_6/\langle 2\rangle$

(G) Look at $\mathrm{Z}_2[x]/\langle x+1\rangle$. All the polys in $\mathrm{Z}_2[x]$ fall into two classes: those with an even # non zero terms (and these are in $\langle x+1\rangle$ by the remainder theorem, and the rest, which are in $1+\langle x+1\rangle$ by the remainder theorem). Thus $\mathrm{Z}_2[x]/\langle x+1\rangle \cong \mathrm{Z}_2$.

We also have:

Theorem 6.6 (**Isomorphism Theorem**)
Let $f\colon R \longrightarrow R'$ be a ring homomorphism. Then there is a natural ring isomorphism

$$\phi\colon R/\ker f \cong \mathrm{Im} f.$$

Examples 6.7

(A) $K[x]/\langle x\rangle \cong K$ (B) $K[x]/\langle x-1\rangle \cong K$

(C) $\mathrm{Z}_p[x]/\langle x-1\rangle \cong \mathrm{Z}_p$

Exercise Set 6

1. Find a subring of $\mathrm{Z}\times\mathrm{Z}$ that is not an ideal.

2. Show that intersections of arbitrary collections of ideals in R are ideals in R.

3. Show that, if I and J are ideals in R, then if L is an ideal containing both I and J, then $I+J \subset L$. (In other words, $I+J$ is the smallest ideal containing I and J.)

4. Prove that every ideal in Z is of the form $n\mathrm{Z}$ for some $n \in \mathrm{Z}$.

5. **Let $a,\ b \in R$. Prove that a divides b iff $bR \subset aR$.**

6. The element $r \in R$ is called **nilpotent** if $r^n = 0$ for some $n \geq 1$. Show that the set of all nilpotent elements in a commutative ring form an ideal (called the **radical** of R).

7. Show that, if $J \lhd R$ contains a unit, then $J = R$. Deduce that the only ideals of a field K are $\{0\}$ and K.

8. Define $\pi\colon \mathrm{R}[x] \longrightarrow \mathrm{C}$ by $\pi(\Sigma a_k x^k) = \Sigma a_k i^k$. Show that π is an epimorphism with kernel containing $\langle x^2+1\rangle$. Deduce that C is isomorphic to a quotient of $\mathrm{R}[x]$. (We shall see later that the kernel is exactly $\langle x^2+1\rangle$.)

9. Here's a new ring, the **ring of cyclotomic integers**. Let $n \geq 2$ and let $\omega = e^{2\pi i/n}$. Define $\mathrm{Z}[\omega]$ to be $\{k_0 + k_1\omega + k_2\omega^2 + \ldots + k_{n-1}\omega^{n-1} : k_i \in \mathrm{Z}\}$

(a) Show that $\Phi_n(\omega) = 1 + \omega + \omega^2 + \ldots + \omega^{n-1} = 0$ [Hint: look at the cyclotomic polynomial in the last section.]

(b) Let $f\colon \mathrm{Z}[x] \longrightarrow \mathrm{Z}[\omega]$ be given by $f(p(x)) = p(\omega)$. Show that f is a ring homomorphism with kernel containing $\langle \Phi_n(x)\rangle$.

(c) Show that, if $n=3$, $\ker f \neq \langle \Phi_n(x)\rangle$ by considering $1 - 2(\omega+\omega^2)$.

7. Maximal and Prime Ideals

Definition 7.1 An ideal $M \lhd R$ is called **maximal** if:

(i) $M \neq R$;
(ii) whenever $M \subset N \lhd R$, then $N = M$ or $N = R$.

Examples 7.2

(A) If p is prime, then $p\mathrm{Z}$ is a maximal ideal in Z. Why? Because if $p\mathrm{Z} \subset q\mathrm{Z} \subset \mathrm{Z}$, then we saw in Lemma 3.1 that q divides p. But, since p is prime, this means that either $q = 1$ or $q = p$, whence $q\mathrm{Z} = p\mathrm{Z}$ or $q\mathrm{Z} = 1\mathrm{Z} = \mathrm{Z}$.
(B) If p is not prime, then $p\mathrm{Z}$ is not maximal. (Exercises)
(C) $\langle x^2+1\rangle$ is maximal in R[x], for essentially the same reason: that x^2+1 is irreducible in R[x].

Theorem 7.3 (Maximal Ideals Yield Fields)
M is maximal in R iff R/M is a field.

Proof:
$\boxed{\square}$: Let M be maximal, and let $a+M \in R/M$ be any non-zero element. ETP it has a multiplicative inverse. But $a+M \neq 0 \Rightarrow a \notin M \Rightarrow \langle a\rangle+M \supsetneqq M$. But, since M is maximal, it follows that $\langle a\rangle+M = R$, whence $1 \in \langle a\rangle+M$. Thus, $1 = ar + m$ for some $r \in R$ and $m \in M$. Passing to equivalence classes, $[1] = [a][r] + [m] = [a][r]+ [0] = [a][r]$.
$\boxed{\square}$: Assume that R/M is a field, and that $M \subset N \lhd R$. If $N \neq M$, then there exists an $n \in N-M$, so that $[n] \neq 0$ in R/M. Since R/M is a field, $[n]$ has an inverse, $[s]$, say. Thus $[ns] = [1]$, so that $ns - 1 \in M$. Write $ns - 1 = m \in M$. But $n \in N$ and N is an ideal, so $ns \in N$. So is m, since $M{\subset}N$. Thus, by the two-out-of-three principle, $1 \in N$. But we have already seen that this implies that $N = R$. ❐

Corollary 7.4 K is a field iff it has no ideals other than $\{0\}$ and K.

Proof: "if" follows from the fact that $\{0\}$ is then a maximal ideal, so $k \cong K/\{0\}$ is a field. "only if" follows from the fact that $K/\{0\}$ is a field, whence $\{0\}$ is maximal. ❐

Definition 7.5 The ideal J in R is called a **prime ideal** if:

(i) $J \neq R$
(ii) $ab \in J \Rightarrow a \in J$ or $b \in J$.

Example 7.6 $p\mathrm{Z}$ is a prime ideal in Z iff p is prime. (Exercises)

The following lemma will prove helpful in doing the above exercise:

Lemma 7.7 (Prime Ideals Yield IDs)
The ideal $J \lhd R$ is prime iff R/J is an integral domain.

Corollary 7.8 Every maximal ideal is prime

Note: The converse of Cor. **7.8** is false in general; see Exercise (5).

Definition The ideal J in R is called **principal** if $J = aR = \langle a\rangle$ for some $a \in R$. R is called a **principal ideal ring** if every ideal is principal.

Examples 7.9

(A) Z (B) $K[x]$ (See Exercise (2))

(C) All fields (since they don't have too many ideals to speak of)

(D) Z[i] (A little beyond the scope of the course, but here is the idea: define $\delta(a+ib) = \sqrt{a^2 + b^2}$. It turns out that a division algorithm works as well as for polynomials, so all the proofs go through.)

Theorem 7.10 (Unique Factorization in $K[x]$)
(a) Every polynomial in $K[x]$ can be written as a product of irreducible polynomials.
(b) The above decomposition is unique up to elements of K. That is, if

$$p(x) = r_1(x)r_2(x) \ . \ . \ . \ r_m(x) = s_1(x)s_2(x) \ . \ . \ . \ s_n(x)$$

are two decompositions into irreducibles (recall that they must have degree ≥ 1), then $m = n$, and, by rearranging the factors, we can assume that, for all i, $r_i(x) = k_is_i(x)$ for some $k_i \in K$.

Part (a) is immediate by the properties of degrees. We prove part (b) by little lemmas.

Lemma 1 If $p(x)$ is irreducible, and $p(x)$ divides $r(x)s(x)$, then either $p(x)$ divides $r(x)$ or $p(x)$ divides $s(x)$.

Proof: Saying that $p(x)$ divides $r(x)s(x)$ is the same as saying that $r(x)s(x) \in \langle p(x)\rangle$. But, since $p(x)$ is irreducible, $\langle p(x)\rangle$ is maximal, and hence prime. Thus, either $r(x)$ or $s(x) \in \langle p(x)\rangle$, and we are done. ❒

Lemma 2 (The inductive step) If

$$p(x) = r_1(x)r_2(x) \ . \ . \ . \ r_m(x) = s_1(x)s_2(x) \ . \ . \ . \ s_n(x)$$

are two decompositions into irreducibles, then $r_1(x) = ks_j(x)$ or some $k \in K$ and some j.

Proof: Since $r_1(x)$ divides the LHS, it divides the RHS, and so, by Lemma 1, it must divide one of the $s_j(x)$'s. Thus, for some j, $s_j(x) = r_1(x)\lambda(x)$. But, since $s_j(x)$ is irreducible, $\lambda(x)$ must be a constant k, and we are done. ❒

Exercise Set 7

1. Show directly that kZ is maximal iff k is prime.

2. **(a)** Prove that if K is a field, then any ideal in $K[x]$ has the form $\langle p(x)\rangle$. [Hint: the proof is exactly the same as the corresponding proof for ideals in Z—use the proof in Exercise Set 6 #4, but using degrees instead of magnitude.]

(b) Deduce the result claimed in Example (C) of maximal ideals by proving the following: **If $p(x)$ is irreducible, then $\langle p(x)\rangle$ is maximal.** [Hint: go through the argument in Example (a) replacing "prime" with "irreducible" and using the bold exercise in Set 6 in place of Lemma 3.1, and replace 1 with a non-zero element of K…]

3. Give a one-line proof that pZ is a prime ideal in Z iff p is prime. [Hint: Use Lemma 7.7 and a result from Exercise Set 2.]

4 Give a one-line proof that all prime ideals of Z are maximal.

5. Show that not every prime ideal of Z×Z is maximal.[Hint: Find quotient of Z×Z that is an integral domain but not a field.]

6. Let K be any field, and let $p(x)$ be an irreducible polynomial in $K[x]$.

(a) Show that $L = K[x]/\langle p(x)\rangle$ is a field containing (a copy of) K. (It is called a **field extension** of K.)

(b) Regarding $p(x)$ as a polynomial over L, show that $p(x)$ has $[x]$ as a zero in L.

(c) Deduce that $p(x)$ has at least one linear factor over L.

(d) Now prove by induction that, if $p(x)$ is any polynomial over K, then there exists a field extension L of K such that $p(x)$ is a product of linear factors in L.

8. Extension Fields

Definition 8.1 A field E is an **extension field** of the field F if $E > F$.

Examples 8.2

(A) C> R > Q (B) Q[$\sqrt{2}$, $\sqrt{3}$] > Q[$\sqrt{2}$] > Q.

(C) The fields in (B) are related by the following diagram:

$$\begin{tikzcd}
& \mathrm{Q}[\sqrt{2}, \sqrt{3}] \arrow[dl, dash] \arrow[dr, dash] & \\
\mathrm{Q}[\sqrt{2}] \arrow[dr, dash] & & \mathrm{Q}[\sqrt{3}] \arrow[dl, dash] \\
& \mathrm{Q} &
\end{tikzcd}$$

Theorem 8.3 (Kronecker)
Let F be any field and let $p(x)$ be any polynomial of degree ≥ 1 over F. Then there exists an extension field E of F such that $p(x)$ has a zero in E.

(Was proved in the last exercise set.)

Examples 8.4

(A) R$[x]/\langle x^2+1\}$ contains both roots of x^2+1. (See Exercise Set 6 #8)

(B) Q$[x]/\langle x^2-2\rangle$ maps onto Q[$\sqrt{2}$] (n fact, isomorphically, as we shall see).

Definition 8.5 Let E be an extension field of F. Then an element $e \in E$ is called **algebraic over *F*** if it is a zero of some polynomial over F. e is called **transcendental over *F*** if it is the solution of no polynomial over F.

Examples 8.6

(A) i, $\sqrt{2}$ are algebraic over Q. (B) e and π are transcendental over Q.

Definition 8.7 A polynomial $p(x) \in F[x]$ is called **monic** if its leading coefficient (i.e., coefficient of the highest power of x) is 1.

Examples: $x + 1$, $x^3 - 45x - 2$, $x^8 + 7x^7$.

Proposition 8.8 (Irreducible Polynomial Associated with and Algebraic Number) Let $a \in E$ be algebraic over F. Then there exists a unique monic polynomial $p(x) \in F[x]$ with the following properties:

(a) $p(a) = 0$ (in E)

(b) $p(x)$ is irreducible in $F[x]$

(c) If $r(x) \in F[x]$ has the property that $r(a) = 0$, then $p(x) \big| r(x)$.

We call $p(x)$ the **irreducible polynomial of *a* over *F***.

Proof. Let ε_a: $F[x] \longrightarrow E$ be the evaluation homomorphism. Its kernel must have the form $\langle p(x) \rangle$ for some monic polynomial $p(x)$. Claim that $p(x)$ satisfies properties (a) through (c). Note that (a) and (c) are immediate. ((c) is immediate, since $r(x) = 0$ iff $r(x) \in \ker\varepsilon_a = \langle p(x) \rangle$.) For (b), Finally, if $p(x) = r(x)s(x)$, then either $r(a) = 0$ or $s(a) = 0$. But if $r(a) = 0$, then $r(x)$ is divisible by $p(x)$ (by part (c)), so that its degree is at least that of p. Therefore $s(x) = constant$. Uniqueness is left as an exercise. Done. ❒

Important Notes 8.9:

(1) If $p(x)$ is any irreducible polynomial over F, then, by Exercise Set 7 #2, $\langle p(x) \rangle$ is maximal, so that $F[x]/\langle p(x) \rangle$ is a field.

(2) If a is algebraic over F, then we saw above that the kernel of ε_a: $F[x] \longrightarrow E$ is $\langle p(x) \rangle$. Thus $F[x]/\langle p(x) \rangle \cong \text{Im}\varepsilon_a$. Since the left-hand side is a field, so is the right-hand side.

(3) Now the image of ε_a has the form $\{f_0 + f_1 a + f_2 a^2 + \ldots + f_r a^r \mid f_i \in F,\ r \in \text{N}\}$, the set of combinations of powers of a with coefficients in F . We denote this field by $F[a]$. (*cf.* Q[$\sqrt{2}$], R[i] = C, etc.)

Definition of *F*[*a*]
If F is a field, and a is algebraic over F, then

$$F[a] = \{k_0 + k_1 a + k_2 a^2 + \ldots + k_r a^r \mid f_i \in F,\ r \in \text{N}\}$$

We have just seen that it is a field. Also, it must be the smallest field extension of F that contains a (by the definition of $F[a]$, and such extension of F must contain $F[a]$...)

(4) $F[a]$ is an extension field of F (since it contains F).

(5) Since $F[a]$ is a field, it follows that the $(f_0 + f_1 a + f_2 a^2 + \ldots + f_r a^r)^{-1}$ is also a linear combination of powers of a! (cf. the inverse of a complex number, or rationalizing the denominator...)

Definition 8.10 Let $a \in E$ be algebraic over F. Then the extension field $F[a]$ is called a **simple extension of *F***. The **degree** of the simple extension $F[a]$ of F is the degree of the irreducible polynomial for a over F. We also refer to this as the **degree of *a* over *F***.

Proposition 8.11 Let a have degree n over F. Then every element of $F[a]$ can be expressed uniquely in the form $f_0 + f_1 a + f_2 a^2 + \ldots + f_{n-1} a^{n-1}$, where $f_i \in F$.

Proof. Let the irreducible monic poly for a over F be

$$p(x) = r_0 + r_1 x + \ldots + r_{n-1} x^{n-1} + x^n.$$

Then, since $p(a) = 0$ in $F[a]$, this permits us to write a^n as a linear combination of lower powers of a. By induction, we can do this for all higher powers. Thus each element of $F[a]$ can be expressed in the form $f_0 + f_1a + f_2a^2 + \ldots + f_{n-1}a^{n-1}$, where $f_i \in F$.
For uniqueness, if

$$f_0 + f_1a + f_2a^2 + \ldots + f_{n-1}a^{n-1}, = g_0 + g_1a + g_2a^2 + \ldots + g_{n-1}a^{n-1},$$

then this would result in a polynomial $s(x)$ of degree $\leq n-1$ with $s(a) = 0$, contradicting the fact that $p(x)$ has the smallest degree among such polynomials, unless $f_i = g_i$ for all i. ❒

Examples 8.12
(A) Look at $R[x]/\langle x^2+1\rangle$. Since $i \in C$ is a root of x^2+1, Important Note (2) tells us that $R[x]/\langle x^2+1\rangle \cong R[i] = C$ (!) This is a result we have long awaited.
(B) Every element of $Q[\sqrt{3}\,]$ has the form $a + b\sqrt{3}$., since $\sqrt{3}$ has degree 2 over Q.

Exercise Set 8
1. Let F be any field of **characteristic** $\boldsymbol{p}$ (p prime). (That is, $p.a = 0$ for every $a \in F$.) Prove that $(x+y)^{p^n} = x^{p^n} + y^{p^n}$ for every n ("sophomore algebra").
2. Prove the uniqueness part of Proposition 8.8.
3 **(a)** Show that $p(x) = x^4 - 2x^2 - 2$ is irreducible over Q. [Hint: Factor it first using the quadratic formula, and then look at all possible factors of degree 1 and 2.]
(b) Show that $a = \sqrt{1+\sqrt{3}}$ is a zero of $p(x)$.
(c) Deduce that $(1+\sqrt{3}\,)^{-1/2}$ can be expressed as a rational combination of $a^0=1$, a, a^2 and a^3.
4 A new finite field with 4 elements
Let $p(x) = x^2 + x + 1 \in Z_2[x]$.
(a) Show that $p(x)$ is irreducible. [Look at all possible linear factors.]
(b) Show that $Z_2[x]/\langle p(x)\rangle$ is a field with exactly 4 elements, and give its multiplication table.
5. Once again, consider the polynomial $p(x) = x^2 + x + 1$. Find all primes $p \leq 10$ such that $p(x)$ is irreducible in $Z_p[x]$, and hence come up with some new fields.
6 Consider the polynomial $p(x) = x^p - x - 1 \in Z_p[x]$ for p prime.
(a) Use Fermat's Little Theorem to show that $p(x)$ has no factors of degree 1.
(b) Deduce that, for every p there exists a field E of order p^n for some $n \geq 2$, and that these fields have the property that $pe = 0$ for all $e \in E$.
(c) Can you push the argument of part (a) further to obtain $n \geq 3$? [Think about possible factorizations of $p(x)$.]
7. Let F be any finite field of characteristic p (p prime). (That is, $p.a = 0$ for every $a \in F$.)
(a) Show that is contains a subfield isomorphic with Z_p.
(b) Prove that each of its elements is algebraic over Z_p. [Look at the group of non-zero elements, and use the fact that it is finite, and so each of its elements has finite order.]
8 Preliminary Classification of Finite Fields. Let E be any finite field.
(a) Show that E contains a copy of Z_p for some prime p.
(b) Show that every simple extension of a finite field F contains $|F|^n$ elements for some n.

(c) Show that every element of E is algebraic over Z_p.
(d) Deduce that every finite field has order p^n for some prime p and integer n.

9. Vector Spaces

Let F be a field.

Definition 9.1 A **Vector space *V* over *F*** is an additive abelian group V together with an operation $F \times V \longrightarrow V$ called **scalar multiplication** such that the following hold for all $v, w \in V$ and $\lambda, \mu \in F$:

$$\lambda(\mu v) = (\lambda\mu)v$$
$$\lambda(v+w) = \lambda v + \lambda w$$
$$(\lambda+\mu)v = \lambda v + \mu v$$
$$1v = v$$

The elements of V are called **vectors**, and the elements of F are called **scalars.**

Examples 9.2

(A) R is a v.s. over R. (B) R^n is a v.s. over R.
(C) F^n is a v.s. over F. (D) C is a v.s. over R.
(E) R is a v.s. over Q.
(F) Any field of characteristic p is a v.s. over Z_p.
(G) $F[x]$ is a v.s. over F. (H) Q[$\sqrt{2}$] is a v.s. over Q.
(I) Any field extension E of F is a v.s. over F.

Lemma 9.3. Let V be a v.s. over F. Then, for all $v \in V$ and $\lambda \in F$,
(a) $0.v = 0$;
(b) $(-\lambda)v = \lambda(-v) = -(\lambda v)$.

Definition 9.4 Let V be a v.s. over F, and let $\{v_\alpha : \alpha \in A\}$ be any collection of vectors. Then the **span** of $\{v_\alpha\}$ is the set $\langle v_\alpha \rangle$ of all *finite* linear combinations of the v_α. We say that$\{v_\alpha\}$ **spans *V*** if $\langle v_\alpha \rangle = V$.

(Henceforth, a "linear combination" is always a finite one.)

Examples 9.5

(A) $\langle e_i \rangle = R^n$ (B) span indep. of row operations.
(C) Finding the span of some vectors in R^4 (in class)
(D) Finding the span of some vectors in C^4 (in class)
(E) Finding the span of some vectors in ${Z_3}^4$ (in class)
(F) If $E = F[a]$ where a is algebraic over F, then E is spanned by powers of a.

Definition 9.6 The v.s. V over F is called **finite dimensional** if it is spanned by some finite set of vectors. Otherwise, it is **infinite dimensional**.

Examples 9.7

(A) F^n over F (B) $F[x]$ is not. (Exercises)
(C) $F[a]$ is f.d. over F for every algebraic element a over F.
(D) R is infinite dimensional over Q. (A cardinality argument)

Definition 9.8 The vectors $\{v_\alpha\}$ are called **linearly independent** if no one of them can be expressed as a linear combination of the others. Equivalently,

$$\lambda_1 v_1 + \lambda_2 v_2 + \ldots + \lambda_r v_r = 0 \text{ implies each } v_i = 0.$$

If they are not independent, then they are **dependent.** Thus dependence implies that some non-trivial linear combination is zero.

Examples 9.9

(A) Vectors in F^n; row reduction test.

(B) If a has degree n over F, then $1, a, a^2, \ldots, a^{n-1}$ are independent, whereas $1, a, \ldots, a^n$ are dependent.

Definition 9.10 A **basis** of the vector space V over F is an independent generating set $\mathcal{B}$.

Theorem 9.11 (Basis Theorem)
The following are equivalent:

(a) $\mathcal{B}$ is a basis for V.
(b) $\mathcal{B}$ is a linearly independent generating set.
(c) $\mathcal{B}$ is a maximal linearly independent set of vectors in V.
(d) $\mathcal{B}$ is a minimal generating set of vectors in V.

Theorem 9.12 (About Bases...)
(a) Every finite generating set of a finite dimensional vector space contains a basis.
(b) Every finite linearly independent set of a f.d. vector space can be enlarged to a basis.
(c) Any two bases for V have the same number of elements

Proof. (a) Start with a finite generating set and keep removing vectors that are linear combinations of others. Eventually, you hit a minimal set (since the original set is finite, so you can't go on forever…) But Theorem 9.11 says that such a minimal set must be a basis.
(b) Start with the linearly indep. set $\mathcal{A}$ and a generating set $\mathcal{G}$ and keep adding vectors from $\mathcal{G}$ to $\mathcal{A}$, not bothering with those that are already in the span of what you have. At each stage, you still have a linearly independent set, so you ultimately wind up with a spanning independent set—i.e., a basis.
(c) If one has more than the other, express each element of the bigger basis $\{b_i\}$ as a linear combination of elements of the smaller. The associated coefficient matrix must reduce to a matrix with at least one row of zeros (since it has too many rows). But this means that some non-trivial linear combination of rows is zero; the same linear combination of the b_i's is therefore also zero, #. ❐

Definition 9.13 The **dimension of V over F** is the size of any basis.

Now let us tun back to extension fields.

Corollary 9.14 (**Degree equals Dimension**)
If the degree of a over F is n, then $\dim F[a] = n$ as a vector space over F. Further, **every element of $F[a]$ is algebraic over F** with degree $\le n$.

Proof. We already know that $\{1, a, a^2, . . . , a^{n-1}\}$ generates $F[a]$. Further, it is a minimal generating set, or else one is in the span of the others, giving a smaller degree polynomial with a as a zero. # Thus it is a basis, and so the dimension is n. For the second part, if $b \in F[a]$, then we must first show that b is algebraic. But consider $\{1, b, b^2, . . . , b^{m-1}, b^n\}$ This can't be linearly independent, since it has too many elements. (See the proof of Theorem 9.3(c) or the exercise set.) Thus some linear combination of them is zero. In other words, b is a zero of some polynomial of degree $\le n$, and thus proves the second part. ❐

Thus we have:

dim $F[a]$ = degree of a's minimal monic poly = the smallest power of a that is a linear combination of the others.

Exercise Set 9

1. Prove that $F[x]$ is infinite dimensional over F.

2. Prove that, if V has a generating set consisting of n vectors, then any set of more than n vectors must be linearly dependent.

3. Prove that a finite dimensional vector space cannot have an infinite basis. [Careful! It is not obvious—look at the definitions—it can conceivably happen. To show that it can't, use Exercise 2.]

4. **General Definition of $F[a]$** Let E be a field extension of F, and let $a \in E-F$. Define $F[a]$ to be the intersection of all subfields $K \subset E$ such that $a \in K \supset F$. Show that $F[a]$ is the smallest subfield of E containing $F\cup\{a\}$. That is, if K is a subfield of E containing $\{a\}$ and F, then $K\supset F[a]$.

5. Prove that a is algebraic over F iff $F[a]$ is finite dimensional over F. [Hint for "if": Assume that a is not algebraic, and that $F[a]$ is finite dimensional. This gives each power of a as a linear combination of some finite generating set of elements of $F[a]$. Use row reduction to argue that some power if a must then be a linear combination of others, and hence obtain a contradiction.

10. Theory of Algebraic Extensions

Definition 10.1 An extension field E of F is an **algebraic extension of F** if each of its elements is algebraic over F.

Examples 10.2

(A) $F[a]$ for a algebraic over F

(B) $(F[a])[b]$ for a algebraic over F and b algebraic over $F[a]$. (See Exercises.)

(C) $F[a_1, a_2, . . . , a_n]$ over F, given that each a_i is algebraic over F.

Definition 10.3 An extension field E of F is a **finite extension of F** if it is finite dimensional as a vector space over F. We denote the degree (dimension) of E over F by $[E{:}F]$.

Proposition 10.4 (What All Finite Extensions Look Like)
All finite extensions are algebraic.

(The converse is not true—see Exercise Set 10.)

We'll only be looking at these very nice kinds of algebraic extensions for a while.

Proposition 10.5 (Dimension of an Extension of an Extension)
If E is a finite extension of F and K is a finite extension of E, then K is a finite extension of F, and

$$\boxed{\boxed{[K{:}F] = [K{:}E][E{:}F]}}$$

Sketch of Proof: If $\{e_i\}$ is a basis for E over F, and $\{k_j\}$ is a basis for K over E, then you just check that $\{e_ij_j\}$ is a basis for K over F by checking the definitions directly (and using the distributive law to get what you want).

Corollary 10.6
(a) This process continues inductively: If F_j is a finite extension of F_{j-1} for $j = 0, \dots,$ n, then F_n is a finite extension of F_0, and

$$[F_n{:}F_0] = \prod_{i=1}^{n} [F_i,F_{i-1}] \ .$$

(b) If $a \in E$ is algebraic over F, and $b \in F[a]$, then the degree of b over F divides the degree of a over F (since $F[b] \subset F[a]$).

Theorem 10.7 (Classification of Finite Extensions)
All finite extensions have the form $F[a_1, a_2, \dots, a_n]$ with each a_i algebraic over F.

Sketch of Proof: Keep selecting elements not in the present filed until you exhaust the finite extension—which you must by 10.6 (a).

Exercise Set 10

1. Show that, if a is algebraic over F and b algebraic over $F[a]$, then $(F[a])[b]$ is algebraic.

2. Show that, if $a_1, a_2, \dots, a_n$ are algebraic over F, then $F[a_1, a_2, \dots, a_n]$ is algebraic over F.

3. Give an example of an algebraic extension of a field F that is not finite. [Hint: If the square of an element of Q[$\sqrt{2}$, $\sqrt{3}$, $\sqrt{5}$, . . . , $\sqrt{p}$] (p prime) is an integer, then it is particularly simple-looking.]

4. Find a basis for each of the following over Q, **justifying your claims**

(a) Q[$2^{1/3}$]

(b) Q[$\sqrt{2}$,$\sqrt{5}$]

(c) Q[$\sqrt{2}$, $\sqrt{3}$, $\sqrt{5}$].

5. Use Corollary 10.6(b) to show that $2^{1/5} \notin$ Q[$2^{1/3}$].

11 You Can't Trisect an Angle

Definition 11.1 A real number α is **constructible with straight-edge and compass** if you can construct a line segment of length $|\alpha|$ in a finite number of steps using a straight-edge ("ruler" in the British terminology) and compass, given a line segment of one unit in length to start with. (After all, you need a scale so that "length" makes sense.)

Proposition 11.2 (Constructible Real Numbers)
The set of all constructible real numbers form a subfield of R (!)

Proof Closure under addition and subtraction is easy. Closure under multiplication and division is shown by using similar triangles. (Take one side of length α, another of length 1, then superimpose a similar triangle with length β, . . .)

Notes

(1) Since it is a field containing 1, it must contain Q as well.

(2) It also contains things like $\sqrt{2}$, using Pythagoras.

In fact:

Lemma 11.3
Let $\mathcal{P}$ be the set of all points in the plane obtainable using a ruler and compass. Then $\mathcal{P}$ consists precisely of all points whose coordinates are constructible.

Proof If a and b are constructible, then you can get a point with coordinates (a, b) using fairly easy constructions. Conversely, if (a, b) can be constructed using compass and ruler, then it is easy to obtain both lengths a and b on the x-axis alone. ❐

Theorem 11.4 (Characterization of Constructible Numbers)
The set of all constructible reals consists of all numbers obtained from rationals by taking square roots and applying field operations successively.

Proof How do you obtain new constructible numbers from old ones? Since you are working in the plane, look at the coordinates. First, you can easily get all points with rational coordinates. Now, to create new points from these using a ruler and compass, you must:

(a) draw an arc with radius equal to the distance between two previously constructed points. (Its equation is then of the form $ax^2 + by^2 + cx + dy + e = 0$, where all the coefficients can be obtained from previously constructed points by using the field operations.)

(b) draw a straight line through two previously constructed points. (Its equation is then $ax + by + c = 0$, where all the coefficients can be obtained from previously constructed points by using the field operations.)

(c) obtain the coordinates of the point of intersection of two of the above curves. The coordinates of the intersection are given by solving a quadratic equation—and this uses only square roots and field operations.

Conversely, it is easy (once you know the trick) to take the square root of a constructible number a geometrically: construct a semicircle of diameter $1+a/4$, and mark off another side with length $1-a/4$. ❒

Corollary 11.5
If a is constructible, then the degree of a over Q is a power of 2.

Proof Adding a square root means extending by a root of a quadratic polynomial. If it's irreducible, then we have a degree 2 extension; if not, then we have a degree $1= 2^0$ extension. Now apply 10.3(a). ❒

Theorem 11.6 (Impossibility of Trisecting and Angle)
It is impossible to trisect an angle with a ruler and compass.

Proof: Now, θ is constructible iff $\cos\theta$ is. (look at a right-triangle with hypotenuse 1. .) Thus, in particular, 60˚ is constructible, since its cosine is. If you could trisect an angle, then you could construct cos 20˚. Now we have the trig identity

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta.$$

Putting $\theta = 20˚$ gives, with $a = \cos 20˚$:

$$\frac{1}{2} = 4a^3 - 3a.$$

Thus a is a zero of the polynomial $p(x) = 8x^3 - 6x - 1$. Claim that it's irreducible over Q. Then we will be done, since the degree of a is then 3, which is not a power of 2, contradicting 11.5. Now, if $p(x)$ is not irreducible, then it also factors over Z. But the only linear factors over Z must have the form $(8x±1)$, $(4x±1)$, $(2x±1)$ or $(x±1)$, and we can check directly that none of these is a factor. ❒

12 Classification of Finite Fields

Throughout, F will be a finite field.

Note

We saw in Section 8 and its exercise set that, if $p \in Z$ is the smallest positive integer such that $p.1 = 0$, then

(a) p is prime.

(b) F is a vector space over Z_p.

(c) $|F| = p^n$, where $n = \dim F$.

We call F a field of **characteristic** $\boldsymbol{p}$.

Theorem 12.1 (Non-zero elements of a Finite Field..)
As a multiplicative abelian group, F^* is cyclic.

Proof By the classification of finite abelian groups,

$$F^* \cong C_{d_1} \times C_{d_2} \ \dots \times C_{d_r}$$

for some integers $d_1, \dots, d_r$. Let m be the lcm of the d_i, so that $m \le d_1 d_2 \dots d_r$. Then, since m is a multiple of the order of every element, one has $x^m = 1$ for every $x \in F^*$. But $x^m - 1$ can have at most m roots, so that we now have

$$|F^*| \le m \le d_1 d_2 \dots d_r = |F^*|,$$

showing that all the inequalities must be equalities, whence $m = d_1 d_2 \dots d_r$, and so the d_i are all relatively prime. Thus, $F \cong C_{d_1} \times C_{d_2} \ \dots \times C_{d_r} \cong C_{d_1 d_2 \dots d_r}$, and we are done. ☯

Corollary 12.2 All finite extensions of finite fields are simple extensions.

Proof Let E be an extension of the finite field F. Then, since E is now also a finite field, E^* is cyclic. Choose $a \in E$ to be a generator of E^*. Then every element of E^* is a power of a, whence $F[a]$ (see section 8 for its definition), being an extension of F that contains every power of a, must contain the whole of E. In other words, $E = F[a]$. ☯

Important Fact From the Proof of Theorem 12.1
If F is a field of order p^n, then every element of F^* is a zero of $x^m - 1$, where m is the lcm of the orders of all the elements of F^*, and also $m = |F^*| = p^n - 1$.

Definition 12.3 If E and E' are extensions of the field F, then we say that E and E' are **isomorphic over F** is there exists a field isomorphism ϕ: $E \cong E'$ such that $\phi(x) = x$ for every $x \in F$. (In other words, $\phi|F = 1_F$, the identity on F.)

Theorem 12.4 (Existence and Uniqueness of GF(p^n))
For every $n \ge 1$, there exists a field of order p^n. Further, and two such fields are isomorphic over Z_p. We denote these fields by GF(p^n).

Proof
Claim 1: The polynomial $p(x) = x^{p^n} - x$ has exactly p^n zeros in the algebraic closure[1] of $\mathbb{Z}_p$.
Proof of Claim 1 In the algebraic closure, we know that $p(x)$ is s product of linear terms,

$$p(x) = \prod_a (x - \alpha) \ ,$$

where these terms may or may not repeat. If the claim is false, then at least one of these terms, α say, repeats. Now take the formal derivative of both sides.[†] Since there is a

[1] The smallest field extension in which ever polynomial has a root. We'll prove the existence of algebraic closure shortly...

repeating root, we must have $D(p(\alpha)) = 0$, by the product rule for the right-hand side. But this implies that $p^n\alpha^{p^n-1} - 1 = 0$. But $\overline{\mathbb{Z}}_p$ is an extension of a field of characteristic p, and thus also has characteristic p, so that $p^n\alpha^{p^n-1} = 0$. But this gives $-1 = 0$ S, establishing the claim.

Existence of GF(p^n)

Let $\alpha_1, \ldots, \alpha_{p^n}$ be the p^n distinct zeros of $p(x) = x^{p^n} - x$ in $\overline{\mathbb{Z}}_p$. Then let

$$E = \{\alpha_1, \ldots, \alpha_{p^n}\}$$

(yes, the *set* of all zeros of $p(x)$).

Claim: E is the desired field.

Proof of This Claim: Closure under ±:

$$(x\pm y)^{p^n} - (x\pm y) = (x^{p^n} - x) \pm (y^{p^n} - y) \text{ (by the sophomore algebra exercise)}$$
$$= 0$$

if x and y are zeros of $p(x)$.

Closure under mult and division:

$$\left(\frac{x}{y}\right)^{p^n} = \frac{x^{p^n}}{y^{p^n}} = \frac{x}{y}$$

if x and y are zeros of $p(x)$, and similarly for multiplication. (It's non-empty since it contains both 1 and 0.)

Uniqueness of GF(p^n)

If F is any other field of order p^n, then we have seen in the Important Fact that each of its elements is a zero of $p(x)$. (Its non-zero elements are all zeros of $x^{p^n-1} - 1$, so multiply this by x.) Thus both F and GF(p^n) are splitting fields for $p(x) \in Z_p[x]$. The fact that they are isomorphic over Z_p now follows by induction on the irreducible factors of $x^{p^n-1} - 1$ from the last proposition in the next section.

❒

Question What does the field structure of the thing look like?

Answer Let α be any generator of F^*. Then every element of F^* is a power of α, so that $\alpha, \alpha^2, \ldots, \alpha^{p^n-1} = 1$ are all distinct., and $F = \{0, \alpha, \alpha^2, \ldots, \alpha^{p^n-1} = 1\}$. Since now F is a simple extension; $F = Z_p[\alpha]$, we have $F \cong Z_p[x]/\langle q(x)\rangle$, where $q(x)$ is irreducible and of degree $\boldsymbol{n}$ (*not* p^n). (How do we come up with this $q(x)$? We look at the kernel of the evaluation-at-α map $Z_p[x] \longrightarrow F$. That kernel includes $x^{p^n-1} - 1$, but is in fact generated by an irreducible $q(x)$ of degree n (showing that $x^{p^n-1} - 1$ is a multiple of $q(x)$).) Once we have our irreducible $q(x)$, we can obtain the structure of F in the usual way (as you did in the exercises using explicit irreducible polynomials.)

[†] **Definition**

D

Error!

Note If $q(x)$ is any irreducible factor of $x^{p^n} - x$, then its degree must be a divisor of n (by the degree theorem) because it will determine an intermediate extension of F. In other words, $x^{p^n} - x$ is a product of irreducible monic polynomials whose degree divides n. Moreover, it is the product of *all* such polynomials. Indeed, if $r(x)$ is one, then look at the extension E of Z_p determined by $r(x)$. It gives a field of order p^s where $s = \delta(r(x))$. Hence $r(x)$ is a divisor of $x^{p^s} - x$. Thus each of its zeros is also a zero of $x^{p^s} - x$. But each zero of $x^{p^s} - x$ is also a zero of $x^{p^n} - x$. (since n a multiple of s implies that $x^{p^n} = (x^{p^s})^{p^s \ldots p^s} = \ldots = x$.) Now is all the zeros of one poly are zeros of another, and if all the zeros are distinct, looking inside the algebraic closure tells us that the one is a factor of the other.

13 Existence of Algebraic Closure

Definition 13.1 A field F is **algebraically closed** if every polynomial completely factors over F. An **algebraic closure** of a field F is a field $\overline{F}$ such that $\overline{F}$ is an algebraic extension of F that is also algebraically closed.

Example 13.2
C is an algebraic closure of R.

Exercise 13.3
$\overline{F}$ is a maximal algebraic extension of F. That is, if $G \supset \overline{F}$ is an algebraic extension of F, then $G = \overline{F}$.

Theorem 13.4 (Existence of Algebraic Closure)
Every field has an algebraic closure.

To prove it, we'll need:

Definition 13.5 A **partial ordering** is a relation $\leq$ that is reflexive, transitive and antisymmetric ($a \leq b$ and $b \leq a \Rightarrow a = b$). A **partially ordered set** (poset) is a set with a partial ordering. If every two elements are comparable (ie., either $a \leq b$, $b \leq a$ or both), then we have an **ordering**.

Examples 13.6
(A) Z, R (B) The set of subsets of any set S.

Definition 13.7 A **chain** in a poset is a collection of elements so that every two are comparable. In other words, it is an ordered subset of a poset.

Example 13.8
(A) Find some chains in the set of subsets of S.

Definition 13.9 If $\mathcal{A}$ is a subset of the poset $\mathcal{P}$, then an **upper bound** of $\mathcal{A}$ is an element $u \in \mathcal{P}$ such that $u \geq a$ for every $a \in \mathcal{A}$. A **maximal** element of the subset $\mathcal{A}$ of $\mathcal{P}$ is an element $a \in \mathcal{A}$ ($\longleftarrow$note) such that $a \leq b \Rightarrow b \notin \mathcal{A}$.

Zorn's Lemma
If $\mathcal{P}$ is a partially ordered set such that every chain in $\mathcal{P}$ has an upper bound in $\mathcal{P}$, then $\mathcal{P}$ has at least one maximal element.

Interesting Corollary 13.10 (Existence of a Basis)
Every vector space has a basis.

Proof Let V be a vector space, take $\mathcal{F}$ to be the poset of linearly independent subsets of V, and let $\mathcal{C}$ be a chain of linearly independent sets. It suffices to show that $\mathcal{C}$ has an upper bound in $\mathcal{F}$. But if $\mathcal{B}$ is the union of the subsets in $\mathcal{C}$, then we claim that $\mathcal{B}$ is independent. Indeed, any finite subset of $\mathcal{B}$ must live in some member of $\mathcal{C}$, and thus be independent. The claim now follows from the fact that a set S is linearly independent iff every finite subset of S is linearly independent. ◆

Proof of Theorem 13.4 in class—follows from Zorn's Lemma. The tricky part is to be able to talk about "the *set* of all algebraic extensions of F." The problem is that the "collection" of all algebraic extensions of F is too big to be a set. What we can do is cut it down a little by looking only at algebraic extensions of F whose elements belong to a prescribed *set* of symbols large enough to include a copy of any algebraic extension. Fraleigh constructs such a set he calls Ω. Here is my own version of Ω: For each irreducible monic polynomial of degree n over F, choose a set of n symbols (to play the role of the no more than n possible zeros x in a polynomial). Let X be the set of all these symbols. Then just take

$$\Omega = X \cup F.$$

If G is an algebraic extension of F, then every element α of G not in F is a zero of some unique monic irreducible poly, and so we can choose one of the n symbols associated with that polynomial to play the role of α. (There are enough of those elements to account for the n possible zeros of the polynomial). In other words, we can choose a copy of G using the symbols in Ω.

Now we are ready to apply Zorn's Lemma: Let $\mathcal{P}$ be the poset (ordered under inclusion) of all algebraic extensions of F that happen to be subsets of Ω (as sets). Then $\mathcal{P}$ contains a copy of every possible algebraic extension of F. Further, the union of a tower of algebraic extensions of F is again an algebraic extension. Thus Zorn's Lemma applies, and there exist maximal algebraic extensions of F. But any maximal algebraic extension of F must be an algebraic closure. ❐

Definition 13.11 Let E be an algebraic extension of F. Then $a, b \in E$ are **conjugate over F** if they are both zeros of the same irreducible polynomial over F.

Proposition 13.12 Let a and b be conjugate over F. Then the map ψ: $F[a]\longrightarrow F[b]$ given by $\psi(\Sigma\lambda_i a^i) = \Sigma\lambda_i b^i$ is a field isomorphism.

Proof This follows from the fact that both are isomorphic with $F[x]/\langle p(x)\rangle$ where $p(x)$ is the irreducible polynomial in question. ❐

Corollary 13.13 If any complex number is a zero of a polynomial with real coefficients, then so is its complex conjugate.

Proof Firstly, i and $-i$ are conjugate according to the above definition, since they are both zeros of the irreducible x^2+1. By the proposition, the map ψ: $a+ib\longrightarrow a-ib$ is therefore a field isomorphism over R. It follows that if $a+ib$ satisfies a poly with real coefficients, then so must $a-ib$ under this field isomorphism ψ. ❐

14 Transcendence of *e*

Recall Definition 8.5: Let E be an extension field of F. Then an element $e \in E$ is called **algebraic over *F*** if it is a zero of some polynomial over F. e is called **transcendental over *F*** if it is the solution of no polynomial over F.

Without more ado, let us prove the

Theorem 14.1 (Transcendence of *e*)
e is transcendental over the rationals.

Proof (Herstein's account of Hurewitz' simplification of Hilbert's proof, which in turn simplifies Hermite's original 1873 proof)
S'pose that e is algebraic, so that is satisfies some equation of the form

$$c_ne^n + c_{n-1}e^{n-1} + \ldots + c_1e + c_0 = 0 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\text{(I)}$$

where $c_i \in Z$ and $c_0 > 0$.

Let p be any prime which is $> c_0$. S'pose we had certain function F_p with the property that $F_p(0)$, .., $F_p(n)$ are integers with $F_p(0) \not\equiv 0 \bmod p$, but $F_p(i) \equiv 0 \bmod p$ for $i \geq 1$. Then I claim that

$$J = c_0F_p(0) + c_1F_p(1) + \ldots + c_nF_p(n)$$

cannot be divisible by p. Indeed, if it were, then, writing $F_p(i) = k_ip$ and substituting yields $c_0F_p(0) \equiv 0 \bmod p$. Thus, since p is prime, wither $p|c_0$ or $p|F_p(0)$. Since $p>c_n$ we can rule out the first possibility, while the second is ruled out by the assumption on the $F_p(i)$.

Now we do a little algebra on the expression J using (I) (which we have not yet used...)

$$\begin{aligned} J &= c_0F_p(0) + c_1F_p(1) + \ldots + c_nF_p(n) \\ &= -(c_ne^n + c_{n-1}e^{n-1} + \ldots + c_1e)F_p(0) + c_1F_p(1) + \ldots + c_nF_p(n) \\ &= c_1[F_p(1)-eF_p(0)] + c_2[F_p(2)-e^2F_p(0)] + \ldots + c_n[F_p(n)-e^nF_p(0)] \\ &= c_1\varepsilon_1 + c_2\varepsilon_2 + \ldots + c_n\varepsilon_n \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\text{(II)} \end{aligned}$$

say.

So far, F_p could be any old functions with the divisibility properties noted above. We now pretend that F_p also have the property that $\varepsilon_i \longrightarrow 0$ as $p \longrightarrow \infty$. Then, for sufficiently large p, we have

$$|J| < 1.$$

But, J, being an integer, cannot have absolute value < 1 unless it is zero. But this makes J divible by p, contradicting the statement in the second paragraph. Hence e is transcendental, provided we can come up with the desired functions F_p. That we can is established in the next set of results. 💣

Notation 14.2 The n,p th polynomial $f_{n,p}(x)$ (due to Hermite) is given by

$$f_{n,p}(x) = \frac{1}{(p-1)!} x^{p-1}(1-x)^p(2-x)^p \ldots (n-x)^p.$$

Lemma 14.3

(a) If $i \geq p$, $\frac{d^i}{dx^i}[f_{n,p}(x)]$ has integer coefficients all divisible by p.

(b) Let $F_p(x) = f_{n,p}(x) + f_{n,p}^{(1)}(x) + \ldots + f_{n,p}^{(r)}(x)$, where r is the degree of $f_{n,p}$. If p is a prime > n, then F_p satisfies the first property we need: $F_p(0), .., F_p(n)$ are integers with $F_p(0) \not\equiv 0 \bmod p$, but $F_p(i) \equiv 0 \bmod p$ for $i \geq 1$.

(c) Let $\varepsilon_i = F_p(i) - e^i F_p(0)$. Then $\varepsilon_i \longrightarrow 0$ as $p \longrightarrow \infty$.

Proof

(a) $f_{n,p}(x)$ has the form $\frac{g(x)}{(p-1)!}$ where $g(x)$ is a polynomial with integer coefficients. The derivatives of order $\geq p-1$ are already integers, because the coefficients are multiples of the binomial coefficients $\binom{r}{p-1}$ (possibly zero) and are therefore integers. If we take a derivative or order p or more, then the coefficients of $\frac{d^i}{dx^i}\frac{g(x)}{p!}$ are also integers (the same argument) whence the coefficients of $\frac{d^i}{dx^i}\frac{g(x)}{(p-1)!} = p\frac{d^i}{dx^i}\frac{g(x)}{p!}$ are divisible by p.

(b) First look at the derivatives of $f_{n,p}$. Since it has a root of multiplicity 2 at 1, 2, ..., n, all the derivatives up through the $(p-1)^{st}$ vanish at $x = 1, 2, \ldots, n$. By part (a), the derivatives of higher order have all their coefficients divisible by p, and hence vanish mod p when they are evaluated. Thus, $F_p(j) \equiv 0 \bmod p$ for $j \geq 1$. It remains to consider $F_p(0)$.

Since 0 is a root of multiplicity $p-1$, all the derivatives through the $p-2$ vanish at 0, and the ones larger than p also vanish mod p. Thus, we worry about the $p-1$ derivative, and look at the coefficient of x^{p-1} (the lowest term). Staring at the polynomial gives the lowest term as

$$\frac{1}{(p-1)!} x^{p-1}(1 \cdot 2^p \cdot \ldots \cdot n^p) = \frac{(n!)^p}{(p-1)!} x^{p-1}.$$

Thus, $f_{n,p}^{(p-1)}(0) = (n!)^p$, which is not divisible by the prime p if $p > n$.

(c) First note that, since

$$F_p(x) = f_{n,p}(x) + f_{n,p}{}^{(1)}(x) + \dots + f_{n,p}{}^{(r)}(x),$$

One has

$$F_p{}^{(1)}(x) - F_p(x) = f_{n,p}{}^{(r+1)}(x) - f_{n,p}(x) = -f_{n,p}(x) \quad \text{..........................} \quad \text{(II)}$$

What about the last assertion: that that $\varepsilon_i \longrightarrow 0$ as $p \longrightarrow \infty$ for $1 \le i \le n$? For that, we need to use the Mean value Theorem, applied to $g(x) = e^{-x}F_p(x)$ over the interval $[0, k]$. The MVT asserts that

$$\frac{g(k) - g(0)}{k-0} = g^{(1)}(k\theta) \text{ for some } \theta \in (0, 1).$$

That is,

$$\frac{e^{-k}F_p(k) - F_p(0)}{k} = -e^{-k\theta}f_{n,p}(k\theta)$$

by (II). A little algebra then gives

$$\begin{aligned}\varepsilon_k = F_p(i) - e^kF_p(0) &= -e^{k(1-\theta)}kf_{n,p}(k\theta) \\ &= -\frac{e^{k(1-\theta)}k(k\theta)^{p-1}(1-k\theta)^p(2-k\theta)^p\dots(n-k\theta)^p}{(p-1)!}\end{aligned}$$

where $0 \le k\theta \le k$ and $1 \le k \le n$. This gives

$$|(1-k\theta)^p(2-k\theta)^p\dots(n-k\theta)^p| \le (n!)^p$$

(This is intuitively clear, since shifting every integer in *n!* to the left by a fixed amount $\le n$ must result in a smaller product. The precise proof is an exercise for you.)
and so

$$|\varepsilon_k| \le e^k\,\frac{n\cdot n^{p-1}(n!)^p}{(p-1)!} = e^k\,\frac{n^p\,(n!)^p}{(p-1)!}\,.$$

For fixed n, a quick look at the ratio test will convince you that $\varepsilon_k \longrightarrow 0$ as $p \longrightarrow \infty$. 💣

Exercise Set 14

1. Prove that, if $1 \le r \le n$, then $|(1-r)(2-r)\dots(n-r)| \le n!$

2. Prove that e is irrational directly, sing its McClaurin series.

3. Prove that e^r is transcendental for every non-zero rational number r.

4. What can you say (if anything) about e^x where x is an arbitrary real number?