A Do It Yourself Guide to Linear Algebra

Lecture Notes based on REUs, 2001-2010

Instructor: László Babai
Notes compiled by Howard Liu

7-2-2010

2 Polynomials and Fields

2.1 Polynomials

The set $\mathbb{R}[x]$ of all polynomials with real coefficients is a vector space.

Exercise 2.1.1. Show that $1, x, x^2, \ldots$ form a basis of $\mathbb{R}[x]$.

Definition 2.1.2. The polynomial $f(x) = \sum a_i x^i$ has **degree** k if $a_k \neq 0$, but $(\forall j > k)(a_j = 0)$. Notation: $\deg(f) = k$. We let $\deg(0) = -\infty$. Note: the nonzero constant polynomials have degree 0.

Exercise 2.1.3. Prove: $\deg(fg) = \deg(f) + \deg(g)$. (Note that this remains true if one of the polynomials f, g is the zero polynomial.)

Exercise 2.1.4. Prove: $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$.

Exercise 2.1.5. Prove that if $f_0, f_1, f_2, \ldots$ is a sequence of polynomials satisfying $\deg(f_i) = i$ then $f_0, f_1, f_2, \ldots$ form a basis of $\mathbb{R}[x]$.

Exercise 2.1.6. Prove: the set of polynomials of degree $\leq n$ forms a subspace of $\mathbb{R}[x]$. Find a basis of this subspace. State the dimension.

Exercise 2.1.7. Let $f(x) = (x - \alpha_1)...(x - \alpha_k)$ where $\alpha_i \neq \alpha_j$ for $i \neq j$. Let $g_i(x) = f(x)/(x - \alpha_i)$. Show that $g_1, \ldots, g_k$ form a basis of the space of polynomials of degree $\leq k - 1$.

2.2 Number Fields

Definition 2.2.1. A subset $F \subseteq \mathbb{C}$ is a **number field** if $1 \in F$ and F is closed under the four arithmetic operations, i.e. for $\alpha, \beta \in F$

(a) $\alpha \pm \beta \in F$

(b) $\alpha\beta \in F$

(c) $\frac{\alpha}{\beta} \in F$ (assuming $\beta \neq 0$).

Exercise 2.2.2. Show that if F is a number field then $Q \subseteq F$.

Exercise 2.2.3. Let $a, b \in \mathbb{Q}$. If $a^2 - 2b^2 = 0$ then $a = b = 0$.

Exercise 2.2.4. Show that the set $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is a number field.

Exercise 2.2.5. Show that the set $\mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Q}\}$ is a number field.

Exercise 2.2.6 (Vector spaces over number fields). Convince yourself that all of the things we have said about vector spaces remain valid if we replace $\mathbb{R}$ by a number field F.

Exercise 2.2.7. Show that if F, G are number fields and $F \subseteq G$ then G is a vector space over F.

Exercise 2.2.8. Show that $\dim_{\mathbb{R}}\mathbb{C} = 2$. What is $\dim_{\mathbb{C}} \mathbb{C}$?

Exercise 2.2.9. Show that $\dim_{\mathbb{Q}}\mathbb{R}$ has the cardinality of "continuum," that is, it has the same cardinality as $\mathbb{R}$.

Exercise 2.2.10. Show that $\dim(F^k) = k$.

Exercise 2.2.11 (Cauchy's Functional Equation). We consider functions $f : \mathbb{R} \to \mathbb{R}$ satisfying Cauchy's Functional Equation: $f(x + y) = f(x) + f(y)$ with $x, y \in \mathbb{R}$. For such a function prove that

(a) If f is continuous then $f(x) = cx$.

(b) If f is continuous at a point then $f(x) = cx$.

(c) If f is bounded on some interval then $f(x) = cx$.

(d) If f is measurable in some interval then $f(x) = cx$.

(e) There exists a $g : \mathbb{R} \to \mathbb{R}$ such that $g(x) \neq cx$ but $g(x + y) = g(x) + g(y)$. (Hint: Use the fact that $\mathbb{R}$ is a vector space over $\mathbb{Q}$. Use a basis of this vector space. Such a basis is called a **Hamel basis**.

Exercise 2.2.12. Show that 1, $\sqrt{2}$, and $\sqrt{3}$ are linearly independent over $\mathbb{Q}$.

Exercise 2.2.13. Show that $1, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{10}, \sqrt{15}$ and $\sqrt{30}$ are linearly independent over $\mathbb{Q}$.

Exercise 2.2.14. * Show that the set of square roots of all of the square-free integers are linearly independent over $\mathbb{Q}$. (An integer is **square free** if it is not divisible by the square of any prime number. For instance, 30 is square free but 18 is not.)

Exercise 2.2.15. $\dim_{\mathbb{R}[x]} \mathbb{R}(x)$ has the cardinality of "continuum" (the same cardinality as $\mathbb{R}$).

2.3 Roots of Unity

Definition 2.3.1. z is a **primitive** n-th root of unity if $z^n = 1$ and $z^j \neq 1$ for $1 \leq j \leq n-1$.

Exercise 2.3.2. Let S_n be the sum of all n-th roots of unity. Show that $S_0 = 1$ and $S_n = 0$ for $n \geq 1$.

Let

$$\zeta_n := \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right) = e^{2\pi i/n}$$

Exercise 2.3.3. $1, \zeta_n, \dots, {\zeta_n}^{n-1}$ are all of the n-th roots of unity.

Exercise 2.3.4. Let $z^n = 1$. Then the powers of z give all n-th roots of unity iff z is a primitive n-th root of unity.

Exercise 2.3.5. Suppose z is a primitive n-th root of unity. For what k is z^k also a primitive n-th root of unity?

Exercise 2.3.6. If z is an n-th root of unity then z^k is also an n-th root of unity.

Definition 2.3.7. The **order** of a complex number is the smallest positive n such that $z^n = 1$. (If no such n exists then we say z has infinite order.)

Example 2.3.8. $\mathrm{ord}(-1) = 2$, $\mathrm{ord}(-\frac{1}{2} + i\frac{\sqrt{3}}{2}) = 3$, $\mathrm{ord}(i) = 4$, $\mathrm{ord}(1) = 1$, $\mathrm{ord}(2) = \infty$.

Exercise 2.3.9. $\mathrm{ord}(z) = n$ iff z is a primitive n-th root of unity.

Exercise 2.3.10. Let $\mu(n)$ be the sum of all primitive n-th roots of unity.

a) Prove that for every n, $\mu(n) = 0, 1$, or -1.

b) Prove $\mu(n) \neq 0$ iff n is square free.

c) Prove if g.c.d. $(k, \ell) = 1$ then $\mu(k\ell) = \mu(k)\mu(\ell)$.

d) If $n = {p_1}^{t_1} \dots {p_k}^{t_k}$, find an explicit formula for $\mu(n)$ in terms of the t_i.

Exercise 2.3.11. Show that the number of primitive n-th roots of unity is equal to Euler's phi function. $\varphi(n) :=$ number of k such that $1 \le k \le n$ and g.c.d. $(k, n) = 1$.

n	1	2	3	4	5	6	7	8	9
$\varphi(n)$	1	1	2	2	4	2	6	4	6

Definition 2.3.12. $f : \mathbb{N}^+ \to \mathbb{C}$ is **multiplicative** if $(\forall k, \ell)$(if g.c.d. $(k, \ell) = 1$ then $f(k\ell) = f(k)f(\ell)$).

Definition 2.3.13. f is **totally multiplicative** if $(\forall k, \ell)(f(k\ell) = f(k)f(\ell))$.

Exercise 2.3.14. The μ function is multiplicative.

Exercise 2.3.15. The φ function is multiplicative.

Exercise 2.3.16. Neither μ nor φ are totally multiplicative.

Exercise 2.3.17. Prove that $\displaystyle\sum_{d \mid n, 1 \le d \le n} \varphi(d) = n$.

Remark 2.3.18. Let $f : \mathbb{N} \to \mathbb{C}$ be a function ($\mathbb{N} = \{1, 2, 3, \dots\}$). We call

$$g(n) = \sum_{d \mid n, 1 \le d \le n} f(d)$$

the **summation function** of f.

Exercise 2.3.19 (Möbius Inversion Formula). $f(n) = \displaystyle\sum_{d \mid n} \mu\left(\frac{n}{d}\right) g(d)$.

Exercise 2.3.20. f is multiplicative if and only if g is.

Now, using the preceding ideas, we can apply in $\mathbb{Q}[\sqrt[3]{2}]$ the same construction we used in $\mathbb{Q}[\sqrt{2}]$. Let a, b, c be rational numbers, not all zero. Let ω be a primitive third root of unity. Consider

$$\frac{1}{a + \sqrt[3]{2}b + \sqrt[3]{4}c} \cdot \frac{a + \omega\sqrt[3]{2}b + \omega^2\sqrt[3]{4}c}{a + \omega\sqrt[3]{2}b + \omega^2\sqrt[3]{4}c} \cdot \frac{a + \omega^2\sqrt[3]{2}b + \omega\sqrt[3]{4}c}{a + \omega^2\sqrt[3]{2}b + \omega\sqrt[3]{4}c}.$$

Exercise 2.3.21. Show that the denominator in the above expression is rational and non-zero.

Exercise 2.3.22 (Kronecker). Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$ be monic ($a_n = 1$). Suppose all complex roots z of f satisfy $|z| = 1$. Then all complex roots of f are roots of unity.

Exercise 2.3.23. The above statement is false if we drop the assumption that f is monic.

2.4 Modular Arithmetic

Notation 2.4.1. The formula $d \mid n$ denotes the relation "d divides n," i.e.,$(\exists k)(n = dk)$. We write $a \equiv b \pmod{m}$ if $m \mid (a - b)$ ("a is congruent to b modulo m").

Exercise 2.4.2. Prove: congruence modulo m is an equivalence relation on $\mathbb{Z}$. The equivalence classes are called the **residue classes**. We denote the set of modulo m resuide classes by $\mathbb{Z}/m\mathbb{Z}$. There are m residue classes modulo m.

Exercise 2.4.3. Prove: if $a_1 \equiv a_2 \pmod{m}$ and $b_1 \equiv b_2 \pmod{m}$, then $a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$ and $a_1 b_1 \equiv a_2 b_2 \pmod{m}$.

Exercise 2.4.4. Define addition and multiplication on the set of modulo m residue classes by representatives. Show that these operations don't depend on the choice of the representatives (Exercise 2.4.3). This way we will have defined a finite commutative ring structure on $\mathbb{Z}/m\mathbb{Z}$.

Example 2.4.5. $\mathbb{Z}/m\mathbb{Z}$:

$m = 2$:

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

$m = 3$:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\times$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$m = 4$:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Exercise 2.4.6. If $ac \equiv bc \pmod{m}$ and g.c.d. $(c, m) = 1$, then $a \equiv b \pmod{m}$.

Exercise 2.4.7 (Multiplicative inverse). $(\exists x)(ax \equiv 1 \pmod{m}) \iff$ g.c.d. $(a, m) = 1$.

Exercise 2.4.8 (Euler-Fermat congruence). If g.c.d. $(a, m) = 1$ then $a^{\rho(m)} \equiv 1 \pmod{m}$.

2.5 Fields

Definition 2.5.1. A **field** is a set F with 2 operations (addition $+$ and multiplication $\times$), $(\mathbb{F}, +, \times)$ such that $(F, +)$ is an abelian group:

(a1) $(\forall \alpha, \beta \in F)(\exists!\, \alpha + \beta \in F)$, (a2) $(\forall \alpha, \beta \in F)(\alpha + \beta = \beta + \alpha)$ (commutative law),

(a3) $(\forall \alpha, \beta, \gamma \in F)((\alpha + \beta) + \gamma = \alpha + (\beta + \gamma))$ (associative law),

(a4) $(\exists 0 \in F)(\forall \alpha)(\alpha + 0 = 0 + \alpha = \alpha)$ (existence of zero),

(a5) $(\forall \alpha \in F)(\exists (-\alpha) \in F)(\alpha + (-\alpha) = 0)$,

and $(F, \times)$ satisfies the following. $F^\times = F \setminus \{0\}$ is an abelian group with respect to multiplication:

(b1) $(\forall \alpha, \beta \in F)(\exists!\, \alpha\beta \in F)$,

(b2) $(\forall \alpha, \beta \in F)(\alpha\beta = \beta\alpha)$ (commutative law),

(b3) $(\forall \alpha, \beta, \gamma \in F)((\alpha\beta)\gamma = \alpha(\beta\gamma))$ (associative law),

(b4) $(\exists 1 \in F)(\forall \alpha)(\alpha \times 1 = 1 \times \alpha = \alpha)$ (existence of identity),

(b5) $(\forall \alpha \in F^\times)(\exists (\alpha^{-1} \in F^\times)(\alpha(\alpha^{-1}) = (\alpha^{-1})\alpha = 1)$,

(b6) $1 \neq 0$

(b7) $(\forall \alpha, \beta, \gamma \in F)((\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma)$ (distributive law)

Example 2.5.2. Examples of fields:

(1) Number fields (every number field is a field)

(2) $\mathbb{R}(x)$, the set of "rational functions"

(3) For prime p, $\mathbb{Z}/p\mathbb{Z}$ is a field, denoted by $\mathbb{F}_p$.

Exercise 2.5.3. If $F = \mathbb{F}_p$ and V is a k-dimensional vector space over F, then $|V| = p^k$.

Axiom (c) (**"no zero divisors"**)

$$(\forall \alpha, \beta \in F)(\alpha\beta = 0 \iff \alpha = 0 \text{ or } \beta = 0)$$

Exercise 2.5.4. Prove that Axiom (c) holds in every field.

Exercise 2.5.5. Show that Axiom (c) fails in $\mathbb{Z}/6\mathbb{Z}$. So $\mathbb{Z}/6\mathbb{Z}$ is not a field.

Exercise 2.5.6. If F is <u>finite</u> and satisfies all field axioms except possibly (b5), then (b5) $\iff$ (c). In other words, if F is a finite commutative ring, $|F| \geqslant 2$ and F has no zero divisors, then F is a field. Note: (c) does **not** necessarily imply (b5) if $\mathbb{F}$ is infinite: $\mathbb{Z}$ is a counterexample.

Theorem 2.5.7. *$\mathbb{Z}/m\mathbb{Z}$ is a field $\iff$ m is prime.*

Proof:

(1) If m is composite, i.e., $m = ab$ where $a, b > 1$, then $\mathbb{Z}/m\mathbb{Z}$ is not a field: it violates axiom (c) because $ab = 0$.

(2) $\mathbb{Z}/p\mathbb{Z}$ is finite, thus need to show that it satisfies axiom (c): This follows from the **prime property:** if p is a prime and $p \mid ab$ then $p \mid a$ or $p \mid b$.

2.6 The "Number Theory" of Polynomials

Definition 2.6.1. Let F be a field. $F[x]$ denotes the set of all univariate polynomials with coefficients in F.

Definition 2.6.2. Let $f, g \in \mathbb{F}[x]$. We say f **divides** g if $(\exists h)(fh = g)$. Notation: $f \mid g$.

Exercise 2.6.3 (Division Theorem). For all $f, g \in F[x])$, if $g \neq 0$, then $(\exists!\, q, r \in F[x])(f = gq + r)$ and $\deg(r) < \deg(g))$.

Notation 2.6.4. $F^\times = F \setminus \{0\}$.

Definition 2.6.5. $f \in F[x]$ is a **unit** if $(\forall g \in F[x])(f \mid g)$.

Exercise 2.6.6. f is a unit $\iff f \mid 1 \iff f$ is a nonzero constant, i.e., $f \in F^\times$.

Definition 2.6.7. For $f, g, h \in F[x]$, f is a **greatest common divisor** (g.c.d.) of g and h if

(1) $f \mid g$ and $f \mid h$.

(2) $(\forall e \in F[x])($ if $e \mid g$ and $e \mid h$ then $e \mid f)$.

Exercise 2.6.8. (1) $(\forall f, g \in F[x])(\exists d \in F[x])(d$ is a g.c.d. of f and $g)$.

(2) d is unique up to multiplication by a unit.

(3) $(\exists u, v \in F[x])(d = fu + gv)$.

Exercise 2.6.9. g.c.d. $(fg, fh) = fd$, where $d =$ g.c.d. (g, h).

Definition 2.6.10. f is **irreducible** over F if

(1) $\deg(f) \geq 1$ and

(2) $(\forall g, h \in \mathbb{F}[x])(f = gh \Rightarrow \deg(f) = 0$ or $\deg(g) = 0)$.

Remark 2.6.11. If $\deg(f) = 1$, then f is irreducible because degree is additive.

Exercise 2.6.12 (Prime property). If f is irreducible and $f \mid gh$ then $f \mid g$ or $f \mid h$. (Hint: Exercise 2.6.9.)

Exercise 2.6.13 (Unique factorization). Every polynomial over F can be uniquely written as a product of irreducible polynomials.

Exercise 2.6.14. $(\forall\alpha)(x-\alpha) \mid (f(x)-f(\alpha))$. Hint: If $f(x)=x^n$, then

$$x^n-\alpha^n=(x-\alpha)(x^{n-1}+\alpha x^{n-2}+...+\alpha^{n-1}).$$

Corollary 2.6.15. *α is a root of f iff $(x-\alpha) \mid f(x)$.*

Theorem 2.6.16 (Fundamental Theorem of Algebra). *If $f \in \mathbb{C}[x]$ and $\deg(f) \geq 1$ then $(\exists\alpha \in \mathbb{C})(f(\alpha)=0)$.*

Exercise 2.6.17. Over $\mathbb{C}$ a polynomial is irreducible iff it is of degree 1. Hint: Follows from the FTA and Corollary 2.6.15 that lets you pull out root factors $(x-\alpha)$.

Exercise 2.6.18. $f(x)=ax^2+bx+c, a \neq 0$, is irreducible over $\mathbb{R}$ iff $b^2-4ac<0$.

Remark 2.6.19. An odd degree polynomial over $\mathbb{R}$ always has a real root.

Exercise 2.6.20. If $f \in \mathbb{R}[x]$, and $z \in \mathbb{C}$, then $f(\bar{z})=\overline{f(z)}$.

Consequence: If z is a root of $f \in \mathbb{R}[x]$ then so is $\bar{z}$.

Theorem 2.6.21. *Over $\mathbb{R}$, all irreducible polynomials have $\deg \leq 2$.*

Proof: Suppose $f \in \mathbb{R}[x]$, $deg(f) \geq 3$. We want to show that f is not irreducible over $\mathbb{R}$.

(1) If f has a real root α, then $(x-\alpha) \mid f$.

(2) Otherwise by FTA f has a complex root z which is not real, so that $z \neq \bar{z}$. Thus $(x-z)(x-\bar{z})=x^2-2ax+a^2+b^2$ divides f, where $z=a+bi$. □

Definition 2.6.22. $f(x)=a_0+a_1x+\cdots+a_nx^n \in \mathbb{Z}[x]$ is a **primitive polynomial** if $\text{g.c.d.}\,(a_0,\ldots,a_n)=1$.

Examples of primitive polynomials: x^n-2; $15x^2+10x+6$. Note that in the second example, every pair of coefficients has a nontrivial common divisor, but the three coefficients together don't.

Exercise 2.6.23 (No zero divisors)**.** For any field F, if $f,g \in F[x]$ then $fg=0 \iff f=0$ or $g=0$.

Exercise 2.6.24 (Gauss Lemma #1). If f,g are primitive polynomials, then so is fg. (Hint: use the preceding exercise.)

Exercise 2.6.25 (Gauss Lemma #2). If $f=gh, f \in \mathbb{Z}[x], g,h \in \mathbb{Q}[x]$ then $\exists\alpha \in \mathbb{Q}$ such that $\alpha g \in \mathbb{Z}[x]$ and $\frac{h}{\alpha} \in \mathbb{Z}[x]$. So if $f \in \mathbb{Z}[x]$ factors nontrivially over $\mathbb{Q}$ then it factors nontrivially over $\mathbb{Z}$.

Exercise 2.6.26 (Rational Root Theorem). Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$ with $a_i \in \mathbb{Z}$, and $\alpha = \frac{r}{s} \in \mathbb{Q}$ with g.c.d. $(r, s) = 1$. If $f(\alpha) = 0$, then $r \mid a_0$ and $s \mid a_n$.

Theorem 2.6.27 (Schönemann-Eisenstein Criterion). *Let $f \in \mathbb{Z}[x], f(x) = a_0 + a_1x + \cdots + a_nx^n$. Assume there exists a prime p such that*

(a) $p \nmid a_n$.

(b) $p \mid a_0, \ldots, a_n$.

(c) $p^2 \nmid a_0$.

Then f is irreducible over $\mathbb{Q}$.

Exercise 2.6.28. Prove the Schönemann-Eisenstein Criterion. Hint: use unique factorization in $\mathbb{F}_p[x]$ (Exercise 2.6.13).

Exercise 2.6.29. If $a_1, \ldots, a_n$ are distinct integers, then $\displaystyle\prod_{i=1}^{n}(x - a_i) - 1$ is irreducible over $\mathbb{Q}$.

Exercise 2.6.30. If $a_1, \ldots, a_n$ are distinct integers, then $\displaystyle\prod_{i=1}^{n}(x - a_i)^2 + 1$ is irreducible over $\mathbb{Q}$.

Exercise 2.6.31. $(\forall n)(x^n - 2$ is irreducible over $\mathbb{Q})$.

Exercise 2.6.32. Let p be a prime. Show that $\Phi_p(x) := \frac{x^p-1}{x-1} = 1+x+\cdots+x^{p-1}$ is irreducible. (Hint: use Schönemann-Eisenstein.)

Definition 2.6.33. The **formal derivative** of $f(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$ (over any field F) is defined as $f'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1}$.

Exercise 2.6.34 (Linearity of differentiation). $(f + g)' = f' + g'$.

Exercise 2.6.35 (Product rule). $(\alpha f)' = \alpha f'$, and $(fg)' = f'g + fg'$.

Exercise 2.6.36 (Chain Rule). If $h(x) = f(g(x))$, then $h'(x) = f'(g(x))g'(x)$.

Exercise 2.6.37. $\alpha \in F$ is a **multiple root** of $f \iff f(\alpha) = f'(\alpha) = 0$.

Exercise 2.6.38. $f \in \mathbb{C}[x]$ has no multiple roots $\iff$ g.c.d. $(f, f') = 1$.

Exercise 2.6.39. Prove that the polynomial $x^n + x + 1$ has no multiple roots in $\mathbb{C}$ for $n \geqslant 2$.

2.7 Cyclotomic Polynomials

Definition 2.7.1. The n-th **cyclotomic polynomial** is $\Phi_n(x) = \prod(x - \zeta)$, where ζ ranges over the primitive n-th roots of unity.

Remark 2.7.2. $\deg \Phi_n(x) = \varphi(n)$.

$$\Phi_1(x) = x - 1$$
$$\Phi_2(x) = x + 1$$
$$\Phi_3(x) = x^2 + x + 1$$
$$\Phi_4(x) = x^2 + 1$$
$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$$
$$\Phi_6(x) = x^2 - x + 1$$
$$\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$
$$\Phi_8(x) = x^4 + 1$$

Exercise 2.7.3. $x^n - 1 = \displaystyle\prod_{d \mid n, 1 \le d \le n} \Phi_n(x)$.

Exercise 2.7.4. Show that $\Phi_n(x) \in \mathbb{Z}[x]$.

Exercise 2.7.5. Show that for primes p, q, $\Phi_p(x) = \frac{x^p-1}{x-1}$, $\Phi_{p^k}(x) = \frac{x^{p^k}-1}{x^{p^{k-1}}-1}$, and $\Phi_{pq}(x) = \frac{(x^{pq}-1)(x-1)}{(x^p-1)(x^q-1)}$.

Theorem 2.7.6. * $\Phi_n(x)$ *is irreducible over* $\mathbb{Q}$*. (We proved this when* n *is prime, Exercise 2.6.32.)*

2.8 Minimal Polynomials

Definition 2.8.1. $\alpha \in \mathbb{C}$ is **algebraic** if $(\exists f)(f \in \mathbb{Q}[x], f \neq 0, f(\alpha) = 0)$. Numbers that are not algebraic are called **transcendental numbers**.

Exercise 2.8.2. (a) Prove that every rational number is algebraic.

(b) Prove: $\sqrt{2}$, $\frac{1+\sqrt{5}}{2}$ (the **golden ratio**), $\sqrt[3]{2}$, $1/(\sqrt{2}+\sqrt{3})$ are algebraic.

(c) Prove: there are only countably many algebraic numbers. So "almost all" real numbers are transcendental.

Very difficult proofs show that e, π, $\ln 2$ are transcendental numbers. It is an open question whether or not $e+\pi$ is transcendental; in fact, it is not even known whether or not $e+\pi$ is irrational.

Definition 2.8.3. A **monic** polynomial is a polynomial with leading coefficient 1.

Definition 2.8.4. The **minimal polynomial** of an algebraic number α is a monic polynomial $m_\alpha(x) \in \mathbb{Q}[x]$ such that

$$m_\alpha(\alpha) = 0 \tag{1}$$

and $m_\alpha(x)$ has minimal degree, among polynomials satisfying (1).

Exercise 2.8.5. $(\forall f \in \mathbb{Q}[x])(f(\alpha) = 0 \iff m_\alpha \mid f)$.

Exercise 2.8.6. The minimal polynomial is unique.

Exercise 2.8.7. $m_\alpha(x)$ is irreducible. In fact, for a monic polynomial f, we have $f = m_\alpha \iff f(\alpha) = 0$ and f is irreducible.

Definition 2.8.8 (degree of an algebraic number). $\deg(\alpha) = \deg(m_\alpha)$.

Exercise 2.8.9. Prove:

(a) $\deg(\sqrt[n]{2}) = n$.

(b) If ζ is a primitive n-th root of unity then $\deg(\zeta) = \varphi(n)$. (This is equivalent to Exercise 2.3.10.)

(c) $\deg(\sqrt{2} + \sqrt{3}) = 4$.

Definition 2.8.10. The **algebraic conjugates** of α are the roots of m_α.

Exercise 2.8.11. Find the algebraic conjugates of the numbers listed in Ex. 2.8.9.

Exercise 2.8.12. If $\deg(\alpha) = n$ then the set

$$\mathbb{Q}[\alpha] := \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_i \in \mathbb{Q}\}$$

is a field.

Exercise 2.8.13. Prove: $\dim_{\mathbb{Q}} \mathbb{Q}[\alpha] = \deg(\alpha)$.

Exercise 2.8.14. Let F be a subfield of the field G. Generalize the definitions above by replacing $\mathbb{Q}$ by F and $\mathbb{C}$ by G. So you will have defined $\deg_F(\alpha)$ for $\alpha \in G$.

Exercise 2.8.15. Prove:

(a) $\deg_{\mathbb{Q}[\sqrt{2}]}(\sqrt{3}) = 2$

(b) $\deg_{\mathbb{Q}[\sqrt{2}]}(\sqrt[3]{2}) = 3$

Exercise 2.8.16. Prove: if $F \subset K \subset L$ are fields then $\dim_F L = (\dim_K L)(\dim_F K)$.

Exercise 2.8.17. Prove: the algebraic numbers form a subfield of $\mathbb{C}$.