Some properties of Natural numbers and Real numbers

1 Preliminaries

Definition 1.1. A binary relation ρ on a nonempty set S is called a *partial order relation* if

1. $a\rho a$ for all $a \in S$ (reflexivity),
2. $a, b \in S$, $a\rho b$ and $b\rho a$ imply $a = b$ (antisymmetry),
3. $a, b, c \in S$, $a\rho b$ and $b\rho c$ imply $a\rho c$ (transitivity).

Definition 1.2. A nonempty set S together with a partial ordering ρ is called a *partially ordered* set. A partially ordered set (S, ρ) is called *totally ordered* if for any $a, b \in S$, either $a\rho b$ or $b\rho a$ or both (in which case $a = b$). A totally ordered set (S, ρ) is called *well-ordered* if every nonempty subset of S has a smallest element.

Definition 1.3. Let $(S, \leq)$ be a partially ordered set (please do not confuse $\leq$ with its usual meaning in $\mathbb{R}$, here $\leq$ is just a replacement for ρ above for convenience). Let A be a nonempty subset of S. An element $x \in S$ is called an *upper bound* of A if $a \leq x$ for all $a \in A$. An upper bound s of A is called the *least upper bound* (in brief, *lub*) or *supremum* (in brief, *sup*) if $s \leq x$ for any upper bound x of A. An element $y \in S$ is called a *lower bound* of A if $y \leq a$ for all $a \in A$. A lower bound t of A is called the *greatest lower bound* (in brief, *glb*) or *infimum* (in brief, *inf*) if $y \leq t$ for any lower bound y of A. An lub (or glb), if it exists, is unique by definition. In this context, we just mention, a partially ordered set is called a *lattice* if there exist lub and glb for every pair of elements in the set. Let A be a nonempty subset of S. If A has an upper bound in S, then A called *bounded above* and if A has a lower bound in S, then A is called *bounded below.* A is called *bounded* if it is both bounded above and bounded below. A totally ordered set $(S, \leq)$ is said to have the *lub property* if every subset A of S which is bounded above has an lub (in S). Similarly, a totally ordered set $(S, \leq)$ is said to have the *glb property* if every subset A of S which is bounded below has a glb (in S).

Definition 1.4. A nonempty set F together with two binary operation $+$ and $\cdot$ is called a *field* if the following conditions are satisfied ($+$ and $\cdot$ are binary operations on F imply that $a+b, a\cdot b \in F$ for all $a, b \in F$):

1. $a + b = b + a$ for all $a, b \in F$,
2. $a + (b + c) = (a + b) + c$ for all $a, b, c \in F$,
3. there exists $0 \in F$ such that $a + 0 = a$ for all $a \in F$,

4. for each $a \in F$, there exists $-a \in F$ such that $a + (-a) = 0$,

5. $a \cdot b = b \cdot a$ for all $a, b \in F$,

6. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in F$,

7. there exists $1 \in F$ such that $a \cdot 1 = a$ for all $a \in F$,

8. for each $0 \neq a \in F$, there exists $a^{-1} \in F$ such that $a \cdot a^{-1} = 1$,

9. $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in F$.

Notations: We denote the sets of natural numbers, integers, rational numbers and real numbers by $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ respectively.

Here we assume the constructions of $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ and the following properties:

1. $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ are totally ordered with usual $\leq$.

2. $(\mathbb{N}, +, \cdot)$ is a totally ordered additively and multiplicatively commutative *semiring* with multiplicative identity (satisfying 1,2,5,6,7,9 of Definition 1.4).

3. $(\mathbb{Z}, +, \cdot)$ is a totally ordered commutative *ring* with identity (satisfying 1,2,3,4,5,6,7,9 of Definition 1.4).

4. $(\mathbb{Q}, +, \cdot)$ a totally ordered field.

5. $(\mathbb{R}, +, \cdot)$ is a totally ordered field with lub property.

Theorem 1.5. *$\mathbb{N}$ is well-ordered, i.e., every nonempty subset of natural numbers contains a smallest element.*

Proof. Let $\emptyset \neq A \subseteq \mathbb{N}$. If $A = \mathbb{N}$, then 1 is the smallest element of A. Let $A \subsetneq \mathbb{N}$. Let $P = \{x \in \mathbb{N} \mid x \leq n \text{ for all } n \in A\}$. Now $P \neq \emptyset$ as $1 \in P$. Then if $x \in P \implies x + 1 \in P$, then by induction $P = \mathbb{N}$ which implies $A = \emptyset$, for otherwise, if $n \in A$, then $n + 1 \notin P = \mathbb{N}$ which is a contradiction. Thus there exists $x_0 \in P$ such that $x_0 + 1 \notin P$. Then there exists $n_0 \in A$ such that $x_0 + 1 > n_0$. Then $x_0 + 1 \geq n_0 + 1$, i.e., $x_0 \geq n_0$. Again $x_0 \leq n_0$ as $x_0 \in P$ and $n_0 \in A$. So $x_0 = n_0 \in A$ and $x_0 \leq n$ for all $n \in A$ as $x_0 \in P$. Therefore x_0 is the least element of A. □

2 Cardinal numbers

Definition 2.1. Let $\mathscr{C}$ be a collection of sets. Define a binary relation $\sim$ on $\mathscr{C}$ by $A \sim B$ if and only if there exists a bijective map from A onto B. It is easy to see that $\sim$ is an equivalence relation on $\mathscr{C}$. For any $A \in \mathscr{C}$, the equivalence class, $\{B \in \mathscr{C} \mid B \sim A\}$ of A under the equivalence relation $\sim$ is said to be the *cardinal number* of A and is denoted by $|A|$. Two sets A and B are said to

be *numerically equivalent* if $A \sim B$, i.e., $|A| = |B|$. For convenience, we write $n = |\{1, 2, \ldots, n\}|$ for any $n \in \mathbb{N}$. A set A is called *finite* if $|A| = n$, i.e., if there exists a bijective map from A onto $\{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$. A set is *infinite* if it is not finite, i.e., if there does not exist a bijective map from A onto $\{1, 2, \ldots, n\}$ for any $n \in \mathbb{N}$. A cardinal number is said to be *infinite* (resp. *finite*) if it is the cardinal number of an infinite set (resp. finite set). The cardinal number of $\mathbb{N}$ is denoted by $\aleph_0$.

Theorem 2.2. (Schroeder-Bernstein Theorem) *Let X and Y be two nonempty sets such that there exist injective maps $f : X \longrightarrow Y$ and $g : Y \longrightarrow X$. Then there exists a bijective map from X onto Y* (for proof, see Simmons Pg 29–30).

Definition 2.3. Let $\mathscr{C}$ be a collection of sets. Define $|A| \leq |B|$ if and only if there exists an injective map from A into B. Then by Schroeder-Bernstein Theorem, we have $\leq$ is a partial order relation on $\mathscr{C}$. We write $|A| < |B|$ if $|A| \leq |B|$ and $|A| \neq |B|$, i.e., if there exists an injective map from A into B, but there does not exist any bijective map from A onto B or, equivalently, there does not exist any injective map from B into A. For example, $|A| < |\mathscr{P}(A)|$ for any set A, where $\mathscr{P}(A)$ denotes the set of all subsets of A. We denote $|\mathscr{P}(A)| = 2^{|A|}$.

Theorem 2.4. (Cardinal Arithmatics) *Let A, B be two sets such that $A \cap B = \emptyset$. Let $\alpha = |A|$ and $\beta = |B|$. Define $\alpha + \beta = |A \cup B|$, $\alpha\beta = |A \times B|$ and $\alpha^\beta = |A^B|$, where A^B denotes the set of all maps from B into A. Then*

1. $\alpha + \beta = \beta + \alpha$, $\alpha\beta = \beta\alpha$
2. $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$, $\alpha(\beta\gamma) = (\alpha\beta)\gamma$.
3. $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$.
4. $\alpha^{(\beta+\gamma)} = \alpha^\beta \cdot \alpha^\gamma$.
5. $(\alpha\beta)^\gamma = \alpha^\gamma \cdot \beta^\gamma$.
6. $(\alpha^\beta)^\gamma = \alpha^{\beta\gamma}$.
7. $\alpha \leq \beta \Longrightarrow \alpha + \gamma \leq \beta + \gamma$, $\alpha\gamma \leq \beta\gamma$, $\alpha^\gamma \leq \beta^\gamma$, $\gamma^\alpha \leq \gamma^\beta$.
8. $\alpha \leq \alpha + \beta$, $\alpha \leq \alpha\beta$.
9. $\alpha < 2^\alpha$.

For all infinite cardinal numbers α, β, the following results hold:

10. $\aleph_0 \leq \alpha$, $n < \alpha$ *for all* $n \in \mathbb{N}$.
11. $\alpha + \alpha = \alpha$, $\alpha\alpha = \alpha$, $n\alpha = \alpha$, $\alpha^n = \alpha$ *for all* $n \in \mathbb{N}$.

12. $\alpha \leq \beta \Longrightarrow \alpha + \beta = \beta$, $\alpha\beta = \beta$. *In particular,* $\aleph_0 + \alpha = \alpha$, $\aleph_0\alpha = \alpha$.

Proof. Below we prove (6). Others are left as exercises.

Let A, B, C be three sets such that $\alpha = |A|$, $\beta = |B|$ and $\gamma = |C|$.
Define the map $\phi : (A^B)^C \longrightarrow A^{B\times C}$ by $\phi(f)(b,c) = f(c)(b)$ for all $b \in B$ and $c \in C$. Note that the maps have the following domains and co-domains: $\phi(f) : B \times C \longrightarrow A$, $f : C \longrightarrow A^B$, $f(c) : B \longrightarrow A$ for all $c \in C$. Now

$$\begin{aligned} & \phi(f_1) = \phi(f_2) \\ \Longrightarrow \quad & \phi(f_1)(b,c) = \phi(f_2)(b,c) \quad \text{for all } b \in B, c \in C \\ \Longrightarrow \quad & f_1(c)(b) = f_2(c)(b) \quad \text{for all } b \in B, c \in C \\ \Longrightarrow \quad & f_1(c) = f_2(c) \quad \text{for all } c \in C \\ \Longrightarrow \quad & f_1 = f_2. \end{aligned}$$

Therefore ϕ is injective.

Let $F \in A^{B\times C}$. Define $f : C \longrightarrow A^B$ by $f(c)(b) = F(b,c)$ for all $b \in B$, $c \in C$. Then

$$\begin{aligned} & c_1 = c_2 \\ \Longrightarrow \quad & (b, c_1) = (b, c_2) \quad \text{for all } b \in B \\ \Longrightarrow \quad & F(b, c_1) = F(b, c_2) \quad \text{for all } b \in B \\ \Longrightarrow \quad & f(c_1)(b) = f(c_2)(b) \quad \text{for all } b \in B \\ \Longrightarrow \quad & f(c_1) = f(c_2). \end{aligned}$$

So f is well-defined. Also $\phi(f)(b,c) = f(c)(b) = F(b,c)$ for all $b \in B$, $c \in C$. Thus $\phi(f) = F$. Therefore ϕ is surjective and hence bijective. So we have $|(A^B)^C| = |A^{B\times C}|$, i.e., $(\alpha^\beta)^\gamma = \alpha^{\beta\gamma}$. □

Definition 2.5. A set is A called *countable* if $|A| \leq \aleph_0$. All finite sets are countable. A countable infinite set is called *countably infinite*. A set A is called *uncountable* if it is not countable ($|A| > \aleph_0$), i.e., if there does not exist any injective map from A into $\mathbb{N}$. The set $\mathbb{R}$ of all real numbers is uncountable. The cardinal number of $\mathbb{R}$ is denoted by c.

Theorem 2.6. *The following results hold:*

1. *Let A be an infinite subset of $\mathbb{N}$. Then $|A| = \aleph_0$.*
2. *Let A be an infinite set and B be a finite set. Then $|A \cup B| = |A|$. If C is a finite subset of A, then $|A \setminus C| = |A|$.*
3. *Let A be an infinite set. Then there exists a subset B of A such that $|B| = |\mathbb{N}|$. That is, every infinite set contains a copy of $\mathbb{N}$.*
4. *A set is infinite if and only if it has a bijection with a proper subset of itself.*

5. *Let* $\{A_i \mid i \in I\}$ *be a collection of sets such that* $|A_i| \leq \aleph_0$*, where* $I \subseteq \mathbb{N}$*. Then* $|\bigcup_{i\in I} A_i| \leq \aleph_0$*. That is, countable union of countable sets is countable.*

6. $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$*, i.e.,* $\aleph_0^2 = \aleph_0$*. In general,* $\aleph_0^n = \aleph_0$ *for all* $n \in \mathbb{N}$*.*

7. *The set* $\mathbb{Z}$ *of all integers and the set* $\mathbb{Q}$ *of all rational numbers are countable, i.e.,* $|\mathbb{Z}| = \aleph_0$ *and* $|\mathbb{Q}| = \aleph_0$*.*

8. *Let* A *be an infinite subset of* $\mathbb{Q}$*, then* $|A| = \aleph_0$*.*

9. $|\mathbb{Q}^n| = \aleph_0$ *for all* $n \in \mathbb{N}$*.* $|\bigcup_{i\in I} A_i| \leq \aleph_0$ *where* $A_i \subseteq \mathbb{Q}$ *for all* $i \in I \subseteq \mathbb{N}$*.*

10. *Let* A, B *be two non-empty sets,* $f : A \longrightarrow B$ *be a surjective map and* A *is countable. Then* B *is also countable, i.e., image of a countable set is countable.*

11. $c > \aleph_0$*, i.e., the set of real numbers is uncountable.*

12. $2^{\aleph_0} = c$*, i.e.,* $|\mathbb{R}| = |\mathscr{P}(\mathbb{N})|$*.*

13. *For any* $a < b$ *in* $\mathbb{R}$*,* $c = |\mathbb{R}| = |(a, b)| = |[a, b]| = |[a, b)| = |(a, b]| = |(0, 1)| = |[0, 1]| = |[0, 1)| = |(0, 1]|$*.*

14. $|\mathbb{N} \times \mathbb{R}| = |\mathbb{Q} \times \mathbb{R}| = |\mathbb{R} \times \mathbb{R}| = |\mathbb{R}^n| = |\mathbb{R}^{\mathbb{N}}| = |\mathbb{R}| = c$ *for all* $n \in \mathbb{N}$*. Note that* $c^{\aleph_0} = c$*.*

15. $|\mathbb{N}^{\mathbb{R}}| = |\mathbb{Q}^{\mathbb{R}}| = |\mathbb{R}^{\mathbb{R}}| = 2^c$*. Note that,* ${\aleph_0}^c = c^c = 2^c$*.*

3 Properties of rational numbers

Theorem 3.1. $\mathbb{Q}$ *is* densely ordered*, i.e., between any two rational numbers, there exist infinite number of rational numbers.*

Hint: $a < \frac{a+b}{2} < b$, $a < \frac{a+\frac{a+b}{2}}{2} < \frac{a+b}{2}$ and so on.

Theorem 3.2. $\mathbb{Q}$ *is* archimedian ordered*, i.e., for any* $a, b \in \mathbb{Q}$ *with* $a, b > 0$*, there exists* $n \in \mathbb{N}$ *such that* $nb > a$*.*

Proof. Suppose $nb \leq a$ for all $n \in \mathbb{N}$. Then $\frac{nb}{a} \leq 1 \leq m$ for all $m, n \in \mathbb{N} \Longrightarrow \frac{n}{m} \leq \frac{a}{b}$ for all $m, n \in \mathbb{N}$ $\Longrightarrow x \leq \frac{a}{b}$ for all $x \in \mathbb{Q}^+$, which is a contradiction (as $\frac{a}{b} + 1 > \frac{a}{b}$). □

Proposition 3.3. $\mathbb{Q}$ *does not have the lub property.*

Proof. Let $A = \{x \in \mathbb{Q} \mid x > 0,\ x^2 < 2\}$. Now A is bounded above as $x < 2$ for all $x \in A$. Let $x \in A$. Define $y = \frac{2x+2}{x+2} = x + \frac{2-x^2}{x+2}$. Since $x^2 < 2$, $y > x$. Also $2 - y^2 = \frac{2(2-x^2)}{(x+2)^2} > 0$. Thus $y^2 < 2$ and so $y \in A$. Therefore for each $x \in A$, there is a y in A such that $y > x$, i.e., A has no greatest element. Again let $B = \{x \in \mathbb{Q} \mid x > 0,\ x^2 > 2\}$. Let $x \in B$. Define $y = x - \frac{x^2-2}{x+2} = \frac{2x+2}{x+2}$. Then $0 < y < x$ and $y^2 > 2$. So B has no least element. Finally, there is no rational number y such that $y^2 = 2$ (surely, its proof is known to you). Thus A has no lub. □

4 Properties of $\mathbb{R}$

Theorem 4.1. *$\mathbb{R}$ is archimedean ordered, i.e., for any $x, y \in \mathbb{R}$ with $x > 0$, there exists $n \in \mathbb{N}$ such that $nx > y$.*

Proof. Let $A = \{nx \mid n \in \mathbb{N}\}$. If the result is not true, then y is an upper bound of A. But then A has a lub in $\mathbb{R}$. Let $\alpha = \sup(A)$. Since $x > 0$, $\alpha - x < \alpha$ and $\alpha - x$ is not an upper bound of A. Then $\alpha - x < mx$ for some $m \in \mathbb{N}$. But then $\alpha < (m+1)x \in A$ which is impossible as $\alpha = \sup(A)$. □

Theorem 4.2. *$\mathbb{Q}$ is dense in $\mathbb{R}$, i.e., if $x, y \in \mathbb{R}$ with $x < y$, then there exists $p \in \mathbb{Q}$ such that $x < p < y$.*

Proof. We have $y - x > 0$. So there exists $n \in \mathbb{N}$ such that $n(y-x) > 1$, i.e., $ny > 1 + nx$ Also $m_1, m_2 \in \mathbb{N}$ such that $m_1 \cdot 1 > nx$ and $m_2 \cdot 1 > -nx$. Then $-m_2 < nx < m_1$. This implies there exists $m \in \mathbb{Z}$ such that $m - 1 \leq nx < m$. Therefore $nx < m \leq 1 + nx < ny$ which imples $x < \frac{m}{n} < y$. This proves the result for $p = \frac{m}{n}$. □

Definition 4.3. (Limit points of a subset of $\mathbb{R}$): Let $S \subseteq \mathbb{R}$ and $x \in \mathbb{R}$. Then x is called a *limit point* of S if for every $\delta > 0$, $(x-\delta, x+\delta) \cap (S \setminus \{x\}) \neq \emptyset$. In other words, every *neighborhood* of x contains at least one point of S different from x itself, where $N \subseteq \mathbb{R}$ is a neighborhood of x if there exists $\delta > 0$, $\delta \in \mathbb{R}$ such that $(x-\delta, x+\delta) \subseteq N$. It is important to understand that δ in the definition of a limit point is arbitrary, i.e., the condition holds for ANY δ (i.e., δ can be as small as you please. But do not romanticize δ to be the length of a very small nano particle! It is simply, arbitrary). Another important thing to note in the definition of a limit point is that $(x-\delta, x+\delta) \cap (S \setminus \{x\}) \neq \emptyset \iff (x-\delta, x+\delta) \cap S$ is infinite (prove!). Finally, note that the limit of a sequence of real numbers is not the same as limit points. For example, the limit of the constant sequence $\{1, 1, 1, \ldots\}$ is 1. But as a set, $\{1, 1, 1, \ldots\} = \{1\}$ and it has no limit points (prove!).

Example 4.4. For example, 0 and 1 are limit points of the set $\{x \in \mathbb{R} \mid 0 < x < 1\}$, i.e., the open interval $(0, 1)$. Note that for any $\delta > 0$, $(-\delta, \delta) \cap (0, 1) \neq \emptyset$ as $0 < \frac{\delta}{2} < \delta < 1$ for $\delta < 1$ and $(0, 1) \subseteq (-\delta, \delta)$ for $\delta \geq 1$. Similarly, $(1-\delta, 1+\delta) \cap (0, 1) \neq \emptyset$ as $0 < 1 - \delta < 1 - \frac{\delta}{2} < 1$ for $\delta < 1$ and $(0, 1) \subseteq (1-\delta, 1+\delta)$ for $\delta \geq 1$. Another example is that 0 is a limit point of set $\left\{\frac{1}{n} \mid n \in \mathbb{N}\right\} = \left\{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \cdots\right\}$ as for any $\delta > 0$, there exists $n \in \mathbb{N}$ such that $0 < \frac{1}{n} < \delta$.

Now which subsets of $\mathbb{R}$ always have limit points? Note that the set $\{1, 2, 3\}$ is finite and bounded, but it has no limits points (prove!). Also $\mathbb{N} = \{1, 2, 3, \ldots\}$ is infinite and not bounded. It has also no limit points (prove!).

Theorem 4.5. *(Bolzano-Weirstrass Theorem) Every bounded infinite subset of $\mathbb{R}$ has a limit point.*

Proof. Let S be a bounded infinite subset of $\mathbb{R}$. Since S is bounded, we have, $S \subseteq [a, b]$ for some $a, b \in \mathbb{R}$ with $a \leq b$. Let $A = \{x \in \mathbb{R} \mid x$ exceeds only a finite number of elements of $S\}$. Now

$A \neq \emptyset$ as $a \in A$. Also A is bounded above. In fact, for all $x \in A$, $x < b$ as for any $y \in \mathbb{R}$ with $y \geq b$ exceeds infinite number of elements of S (in fact, all elements of S and S is infinite). Thus by lub property, A has an lub, say, $r \in \mathbb{R}$.

We show that r is a limit point of S. Let $\delta > 0$. Then $r - \delta \in A$ and $r + \delta \notin A$. Thus $(r-\delta, r+\delta) \cap S$ contains infinite number of elements of S. This implies r is a limit point of S. □

4.1 Decimal expansion of Real numbers

Let $x > 0$, $x \in \mathbb{R}$. Let n_0 be the largest integer such that $n_0 \leq x$.

Having chosen $n_0, n_1, \ldots, n_{k-1}$, let n_k be the largest integer such that $n_0 + \frac{n_1}{10} + \cdots + \frac{n_k}{10^k} \leq x$.

Let $E = \left\{ n_0 + \frac{n_1}{10} + \cdots + \frac{n_k}{10^k} \mid k = 0, 1, 2, 3, \ldots \right\}$. Then $x = \sup(E)$. The decimal expansion of x is given by $n_0.n_1n_2 \ldots n_k \ldots$.

◊ **Exercise 4.1.** Prove that $\mathbb{R}$ has the glb property.

◊ **Exercise 4.2.** Find lub and glb of the following subsets of $\mathbb{R}$:

1. $S = \left\{ 1 + \frac{1}{n} \mid n \in \mathbb{N} \right\}$,
2. $S = \left\{ \frac{n}{n+2} \mid n \in \mathbb{N} \right\}$.

◊ **Exercise 4.3.** Let $\emptyset \neq S, T \subseteq \mathbb{R}$ be two bounded sets. Prove the following:

1. $S \subseteq T \Longrightarrow \inf(T) \leq \inf(S) \leq \sup(S) \leq \sup(T)$.
2. If $M = \{x \in \mathbb{R} \mid -x \in S\}$, then $\sup(M) = -\inf(S)$ and $\inf(M) = -\sup(S)$.
3. If $A = \{x + y \mid x \in S,\ y \in T\}$, then $\sup(A) = \sup(S) + \sup(T)$ and $\inf(A) = \inf(S) + \inf(T)$.
4. If $B = \{|x - y| \mid x, y \in S\}$, then $\sup(B) = \sup(S) - \inf(S)$ and $\inf(B) = 0$.

APPENDIX THREE

Boolean Algebras, Boolean Rings, and Stone's Theorem

We saw in Sec. 2 that a *Boolean algebra of sets* can be defined as a class of subsets of a non-empty set which is closed under the formation of finite unions, finite intersections, and complements. Our purpose in this appendix is threefold: to define abstract Boolean algebras by means of lattices; to show that the theory of these systems can be regarded as part of the general theory of rings; and to prove the famous theorem of Stone, which asserts that every Boolean algebra is isomorphic to a Boolean algebra of sets.

The reader will recall that a *lattice* is a partially ordered set in which each pair of elements x and y has a greatest lower bound $x \wedge y$ and a least upper bound $x \vee y$, and that these elements are uniquely determined by x and y. It is easy to show (see Problem 8-5) that the operations $\wedge$ and $\vee$ have the following properties:

$$x \wedge x = x \quad \text{and} \quad x \vee x = x; \tag{1}$$

$$x \wedge y = y \wedge x \quad \text{and} \quad x \vee y = y \vee x; \tag{2}$$

$$x \wedge (y \wedge z) = (x \wedge y) \wedge z \quad \text{and} \quad x \vee (y \vee z) = (x \vee y) \vee z; \tag{3}$$

$$(x \wedge y) \vee x = x \quad \text{and} \quad (x \vee y) \wedge x = x. \tag{4}$$

We shall see in the next paragraph that these properties are actually characteristic of lattices. Before proceeding further, however, we remark that

$$x \leq y \Leftrightarrow x \wedge y = x.$$

This fact serves to motivate the following discussion.

Let L be a non-empty set in which two operations $\wedge$ and $\vee$ are defined, and assume that these operations satisfy the above conditions. We

shall prove that a partial order relation $\leq$ can be defined in L in such a way that L becomes a lattice in which $x \wedge y$ and $x \vee y$ are the greatest lower bound and least upper bound of x and y. Our first step is to notice that $x \wedge y = x$ and $x \vee y = y$ are equivalent; for if $x \wedge y = x$, then $x \vee y = (x \wedge y) \vee y = (y \wedge x) \vee y = y$, and similarly $x \vee y = y$ implies $x \wedge y = x$. We now define $x \leq y$ to mean that either $x \wedge y = x$ or $x \vee y = y$. Since $x \wedge x = x$, we have $x \leq x$ for every x. If $x \leq y$ and $y \leq x$, so that $x \wedge y = x$ and $y \wedge x = y$, then $x = x \wedge y = y \wedge x = y$. If $x \leq y$ and $y \leq z$, so that $x \wedge y = x$ and $y \wedge z = y$, then

$$x \wedge z = (x \wedge y) \wedge z = x \wedge (y \wedge z) = x \wedge y = x,$$

so $x \leq z$. This completes the proof that $\leq$ is a partial order relation. We now show that $x \wedge y$ is the greatest lower bound of x and y. Since $(x \wedge y) \vee x = x$ and $(x \wedge y) \vee y = (y \wedge x) \vee y = y$, we see that $x \wedge y \leq x$ and $x \wedge y \leq y$. If $z \leq x$ and $z \leq y$, so that $z \wedge x = z$ and $z \wedge y = z$, then $z \wedge (x \wedge y) = (z \wedge x) \wedge y = z \wedge y = z$, so $z \leq x \wedge y$. It is easy to prove, by similar arguments, that $x \vee y$ is the least upper bound of x and y.

This characterization of lattices brings the theory of these systems somewhat closer to ordinary abstract algebra, in which operations (instead of relations) are usually placed in the foreground.

A lattice is said to be *distributive* if it has the following properties:

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z) \tag{5}$$

and

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z). \tag{6}$$

It is useful to know that (5) and (6) are equivalent to one another. For if (5) holds, then

$$\begin{aligned}(x \vee y) \wedge (x \vee z) &= [(x \vee y) \wedge x] \vee [(x \vee y) \wedge z] \\ &= x \vee [(x \vee y) \wedge z] \\ &= x \vee [(x \wedge z) \vee (y \wedge z)] \\ &= [x \vee (x \wedge z)] \vee (y \wedge z) \\ &= x \vee (y \wedge z),\end{aligned}$$

and a similar computation shows that (6) implies (5). We shall say that a lattice is *complemented* if it contains distinct elements 0 and 1 such that

$$0 \leq x \leq 1 \tag{7}$$

for every x (these elements are clearly unique when they exist), and if each element x has a *complement* x' with the property that

$$x \wedge x' = 0 \quad \text{and} \quad x \vee x' = 1. \tag{8}$$

We now define a *Boolean algebra* to be a complemented distributive lattice.

It is quite possible for an element of a complemented lattice to have many different complements. In a Boolean algebra, however, each

CHAPTER 9

Algebraic Numbers

To illustrate one purpose of this chapter, we take a different approach to the equation $x^2 + y^2 = z^2$ than in Section 5.3. Factoring $x^2 + y^2$ into $(x + yi)(x - yi)$, we can write

$$x^2 + y^2 = (x + yi)(x - yi) = z^2.$$

If from this we could conclude that $x + yi$ and $x - yi$ are both squares of complex numbers of the same type, we would have

$$x + yi = (r + si)^2, \qquad x - yi = (r - si)^2.$$

Equating the real and the nonreal parts here gives

$$x = r^2 - s^2, \qquad y = 2rs$$

and so $z = r^2 + s^2$. These are precisely the equations in Theorem 5.5.

The steps in this argument are valid but not quite complete, and they need justification. We shall make the justification and complete the argument in Section 9.9. A similar factoring of $x^3 + y^3$ into three linear factors in complex numbers is used in the last section of the chapter to prove that $x^3 + y^3 = z^3$ has no solutions in positive integers. This is another case of Fermat's last theorem, $x^4 + y^4 = z^4$ having been proved impossible in positive integers in Section 5.4.

However, the analysis of Diophantine equations is just one purpose of this chapter. Algebraic integers are a natural extension of the ordinary integers and are interesting in their own right. The title of this chapter is a little pretentious, because the algebraic numbers studied here are primarily only quadratic in nature, satisfying simple algebraic equations of degree 2. The plan is to develop some general theory in the first four sections and then take up the special case of the quadratic case, where much more can be said than in the general case.

9.1 POLYNOMIALS

Algebraic numbers are the roots of certain types of polynomials, so it is natural to begin our discussion with this topic. Our plan in this chapter is to proceed from the most general results about algebraic numbers to stronger specific results about special classes of algebraic numbers. In this process of proving more and more about less and less, we have selected material of a number theoretic aspect as contrasted with the more "algebraic" parts of the theory. In other words, we are concerned with such questions as divisibility, uniqueness of factorization, and prime numbers, rather than questions concerning the algebraic structure of the groups, rings, and fields arising in the theory.

The polynomials that we shall consider will have rational numbers for coefficients. Such polynomials are called *polynomials over* $\mathbb{Q}$, where $\mathbb{Q}$ denotes the field of rational numbers. This collection of polynomials in one variable x is often denoted by $\mathbb{Q}[x]$, just as all polynomials in x with integral coefficients are denoted by $\mathbb{Z}[x]$, and the set of all polynomials in x with coefficients in any set of numbers F is denoted by $F[x]$. That the set of rational numbers forms a field can be verified from the postulates in Section 2.11. In a polynomial such as

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n, \qquad a_0 \neq 0$$

the nonnegative integer n is called the *degree* of the polynomial, and a_0 is called the *leading* coefficient. If $a_0 = 1$, the polynomial is called *monic*. Since we assign no degree to the zero polynomial, we can assert without exception that the degree of the product of two polynomials is the sum of the degrees of the polynomials.

A polynomial $f(x)$ is said to be *divisible* by a polynomial $g(x)$, not identically zero, if there exists a polynomial $q(x)$ such that $f(x) = g(x)q(x)$ and we write

$$g(x) \mid f(x).$$

Also, $g(x)$ is said to be a *divisor* or *factor* of $f(x)$. The degree of $g(x)$ here does not exceed that of $f(x)$, unless $f(x)$ is identically zero, written $f(x) \equiv 0$. This concept of divisibility is not the same as the divisibility that we have considered earlier. In fact $3 \mid 7$ holds if 3 and 7 are thought of as polynomials of degree zero, whereas it is not true that the integer 3 divides the integer 7.

Theorem 9.1 *To any polynomials $f(x)$ and $g(x)$ over $\mathbb{Q}$ with $g(x) \not\equiv 0$, there correspond unique polynomials $q(x)$ and $r(x)$ such that $f(x) = g(x)q(x) + r(x)$, where either $r(x) \equiv 0$ or $r(x)$ is of lower degree than $g(x)$.*

This result is the *division algorithm for polynomials* with rational coefficients, analogous to the division algorithm for integers in Theorem 1.2. Most of the theorems in this section have analogues in Chapter 1, and the methods used earlier can often be adapted to give proofs here. Although it is stated explicitly in Theorem 9.1 that $f(x)$ and $g(x)$ belong to $\mathbb{Q}[x]$, as do $q(x)$ and $r(x)$, this assumption will be taken for granted implicitly in subsequent theorems.

Proof In case $f(x) \equiv 0$ or $f(x)$ has lower degree than $g(x)$, define $q(x) \equiv 0$ and $r(x) = f(x)$. Otherwise divide $g(x)$ into $f(x)$ to get a quotient $q(x)$ and a remainder $r(x)$. Clearly $q(x)$ and $r(x)$ are polynomials over $\mathbb{Q}$, and either $r(x) \equiv 0$ or the degree of $r(x)$ is less than the degree of $g(x)$ if the division has been carried to completion. If there were another pair, $q_1(x)$ and $r_1(x)$, then we would have

$$f(x) = g(x)q_1(x) + r_1(x), \qquad r(x) - r_1(x) = g(x)\{q_1(x) - q(x)\}.$$

Thus $g(x)$ would be a divisor of the polynomial $r(x) - r_1(x)$, which, unless identically zero, has lower degree than $g(x)$. Hence $r(x) - r_1(x) \equiv 0$, and it follows that $q(x) = q_1(x)$.

Theorem 9.2 *Any polynomials $f(x)$ and $g(x)$, not both identically zero, have a common divisor $h(x)$ that is a linear combination of $f(x)$ and $g(x)$. Thus $h(x)|f(x)$, $h(x)|g(x)$, and*

$$h(x) = f(x)F(x) + g(x)G(x) \tag{9.1}$$

for some polynomials $F(x)$ and $G(x)$.

Proof From all the polynomials of the form (9.1) that are not identically zero, choose any one of least degree and designate it by $h(x)$. If $h(x)$ were not a divisor of $f(x)$, Theorem 9.1 would give us $f(x) = h(x)q(x) + r(x)$ with $r(x) \not\equiv 0$ and $r(x)$ of degree lower than $h(x)$. But then $r(x) = f(x) - h(x)q(x) = f(x)\{1 - f(x)q(x)\} - g(x)\{G(x)q(x)\}$, which is of the form (9.1) in contradiction with the choice of $h(x)$. Thus $h(x)|f(x)$ and similarly $h(x)|g(x)$.

Theorem 9.3 *To any polynomials $f(x)$ and $g(x)$, not both identically zero, there corresponds a unique monic polynomial $d(x)$ having the properties*

(1) $d(x)|f(x)$, $d(x)|g(x)$;

(2) $d(x)$ is a linear combination of $f(x)$ and $g(x)$, as in (9.1);

(3) any common divisor of $f(x)$ and $g(x)$ is a divisor of $d(x)$, and thus there is no common divisor having higher degree than that of $d(x)$.

Proof Define $d(x) = c^{-1}h(x)$, where c is the leading coefficient of $h(x)$, so that $d(x)$ is monic. Properties (1) and (2) are inherited from $h(x)$ by $d(x)$. Equation (9.1) implies $d(x) = c^{-1}f(x)F(x) + c^{-1}g(x)G(x)$, and this equation shows that if $m(x)$ is a common divisor of $f(x)$ and $g(x)$, then $m(x)|d(x)$. Finally, to prove that $d(x)$ is unique, suppose that $d(x)$ and $d_1(x)$ both satisfy properties (1), (2), (3). We then have $d(x)|d_1(x)$ and $d_1(x)|d(x)$, hence $d_1(x) = q(x)d(x)$ and $d(x) = q_1(x)d_1(x)$ for some polynomials $q(x)$ and $q_1(x)$. This implies $q(x)q_1(x) = 1$, from which we see that $q(x)$ and $q_1(x)$ are of degree zero. Since both $d(x)$ and $d_1(x)$ are monic, we have $q(x) = 1$, $d_1(x) = d(x)$.

Definition 9.1 *The polynomial $d(x)$ is called the* greatest common divisor *of $f(x)$ and $g(x)$. We write $(f(x), g(x)) = d(x)$.*

Definition 9.2 *A polynomial $f(x)$, not identically zero, is* irreducible, *or* prime, *over $\mathbb{Q}$ if there is no factoring, $f(x) = g(x)h(x)$, of $f(x)$ into two polynomials $g(x)$ and $h(x)$ of positive degrees over $\mathbb{Q}$.*

For example $x^2 - 2$ is irreducible over $\mathbb{Q}$. It has the factoring $(x - \sqrt{2})(x + \sqrt{2})$ over the field of real numbers, but it has no factoring over $\mathbb{Q}$.

Theorem 9.4 *If an irreducible polynomial $p(x)$ divides a product $f(x)g(x)$, then $p(x)$ divides at least one of the polynomials $f(x)$ and $g(x)$.*

Proof If $f(x) \equiv 0$ or $g(x) \equiv 0$ the result is obvious. If neither is identically zero, let us assume that $p(x) \nmid f(x)$ and prove that $p(x)|g(x)$. The assumption that $p(x) \nmid f(x)$ implies that $(p(x), f(x)) = 1$, and hence by Theorem 9.3 there exist polynomials $F(x)$ and $G(x)$ such that $1 = p(x)F(x) + f(x)G(x)$. Multiplying by $g(x)$ we get

$$g(x) = p(x)g(x)F(x) + f(x)g(x)G(x).$$

Now $p(x)$ is a divisor of the right member of this equation because $p(x)|f(x)g(x)$, and hence $p(x)|g(x)$.

Theorem 9.5 *Any polynomial $f(x)$ over $\mathbb{Q}$ of positive degree can be factored into a product $f(x) = cp_1(x)p_2(x)\cdots p_k(x)$ where the $p_j(x)$ are irreducible monic polynomials over $\mathbb{Q}$. This factoring is unique apart from order.*

Proof Clearly $f(x)$ can be factored repeatedly until it becomes a product of irreducible polynomials, and the constant c can be adjusted to make all

the factors monic. We must prove uniqueness. Let us consider another factoring, $f(x) = cq_1(x)q_2(x)\cdots q_j(x)$, into irreducible monic polynomials. According to Theorem 9.4, $p_1(x)$ divides some $q_i(x)$, and we can reorder the $q_m(x)$ to make $p_1(x)|q_1(x)$. Since $p_1(x)$ and $q_1(x)$ are irreducible and monic, we have $p_1(x) = q_1(x)$. A repetition of this argument yields

$$p_2(x) = q_2(x), \qquad p_3(x) = q_3(x), \cdots, \qquad \text{and } k = j.$$

Definition 9.3 *A polynomial* $f(x) = a_0x^n + \cdots + a_n$ *with integral coefficients* a_j *is said to be* primitive *if the greatest common divisor of its coefficients is* 1. *Obviously, here we mean the greatest common divisor of integers as defined in Definition* 1.2.

Theorem 9.6 *The product of two primitive polynomials is primitive.*

Proof Let $a_0x^n + \cdots + a_n$ and $b_0x^m + \cdots + b_m$ be primitive polynomials and denote their product by $c_0x^{n+m} + \cdots + c_{n+m}$. Suppose that this product polynomial is not primitive, so that there is a prime p that divides every coefficient c_k. Since $a_0x^n + \cdots + a_n$ is primitive, at least one of its coefficients is not divisible by p. Let a_i denote the first such coefficient and let b_j denote the first coefficient of $b_0x^m + \cdots + b_m$, not divisible by p. Then the coefficient of $x^{n+m-i-j}$ in the product polynomial is

$$c_{i+j} = \sum a_k b_{i+j-k} \tag{9.2}$$

summed over all k such that $0 \leqslant k \leqslant n$, $0 \leqslant i + j - k \leqslant m$. In this sum, any term with $k < i$ is a multiple of p. Any term with $k > i$ that appears in the sum will have the factor b_{i+j-k} with $i + j - k < j$ and will also be a multiple of p. The term a_ib_j, for $k = i$, appears in the sum, and we have $c_{i+j} \equiv a_jb_j \pmod{p}$. But this is in contradiction with $p|c_{i+j}$, $p \nmid a_i$, $p \nmid b_j$.

Theorem 9.7 *Gauss's lemma. If a monic polynomial* $f(x)$ *with integral coefficients factors into two monic polynomials with rational coefficients, say* $f(x) = g(x)h(x)$, *then* $g(x)$ *and* $h(x)$ *have integral coefficients.*

Proof Let c be the least positive integer such that $cg(x)$ has integral coefficients; if $g(x)$ has integral coefficients take $c = 1$. Then $cg(x)$ is a primitive polynomial, because if p is a divisor of its coefficients, then $p|c$ because c is the leading coefficient, and $(c/p)g(x)$ would have integral coefficients contrary to the minimal property of c. Similarly let c_1 be least positive integer such that $c_1h(x)$ has integral coefficients, and hence

$c_1 h(x)$ is also primitive. Then by Theorem 9.6 the product $\{cg(x)\}\{c_1 h(x)\} = cc_1 f(x)$ is primitive. But since $f(x)$ has integral coefficients, it follows that $cc_1 = 1$ and $c = c_1 = 1$.

PROBLEMS

1. If $f(x)|g(x)$ and $g(x)|f(x)$, prove that there is a rational number c such that $g(x) = cf(x)$.
2. If $f(x)|g(x)$ and $g(x)|h(x)$, prove that $f(x)|h(x)$.
3. If $p(x)$ is irreducible and $g(x)|p(x)$, prove that either $g(x)$ is a constant or $g(x) = cp(x)$ for some rational number c.
4. If $p(x)$ is irreducible, prove that $cp(x)$ is irreducible for any rational $c \neq 0$.

*5. If a polynomial $f(x)$ with integral coefficients factors into a product $g(x)h(x)$ of two polynomials with coefficients in $\mathbb{Q}$, prove that there is a factoring $g_1(x)h_1(x)$ with integral coefficients.

6. If $f(x)$ and $g(x)$ are primitive polynomials, and if $f(x)|g(x)$ and $g(x)|f(x)$, prove that $f(x) = \pm g(x)$.
7. Let $f(x)$ and $g(x)$ be polynomials in $\mathbb{Z}[x]$, that is, polynomials with integral coefficients. Suppose that $g(m)|f(m)$ for infinitely many positive integers m. Prove that $g(x)|f(x)$ in $\mathbb{Q}[x]$, that is, there exists a quotient polynomial $q(x)$ with rational coefficients such that $f(x) = g(x)q(x)$. (*Remark*: The example $g(x) = 2x + 2$, $f(x) = x^2 - 1$ with m odd shows that $q(x)$ need not have integral coefficients.) (H)
8. Let $f(x)$ and $g(x)$ be primitive nonconstant polynomials in $\mathbb{Z}[x]$ such that the greatest common divisor $(f(m), g(m)) > 1$ for infinitely many positive integers m. Construct an example to show that such polynomials exist with g.c.d.$(f(x), g(x)) = 1$ in the polynomial sense.
9. Given any nonconstant polynomial $f(x)$ with integral coefficients, prove that there are infinitely many primes p such that $f(x) \equiv 0 \pmod{p}$ is solvable. (H)

9.2 ALGEBRAIC NUMBERS

Definition 9.4 *A complex number ξ is called an* algebraic number *if it satisfies some polynomial equation $f(x) = 0$ where $f(x)$ is a polynomial over $\mathbb{Q}$.*

Every rational number r is an algebraic number because $f(x)$ can be taken as $x - r$ in this case.

Any complex number that is not algebraic is said to be *transcendental*. Perhaps the best known examples of transcendental numbers are the familiar constants π and e. At the end of this section, we prove the existence of transcendental numbers by exhibiting one, using a very simple classical example.

Theorem 9.8 *An algebraic number ξ satisfies a unique irreducible monic polynomial equation $g(x) = 0$ over $\mathbb{Q}$. Furthermore, every polynomial equation over $\mathbb{Q}$ satisfied by ξ is divisible by $g(x)$.*

Proof From all polynomial equations over $\mathbb{Q}$ satisfied by ξ, choose one of lowest degree, say $G(x) = 0$. If the leading coefficient of $G(x)$ is c, define $g(x) = c^{-1}G(x)$, so that $g(\xi) = 0$ and $g(x)$ is monic. The polynomial $g(x)$ is irreducible, for if $g(x) = h_1(x)h_2(x)$, then one at least of $h_1(\xi) = 0$ and $h_2(\xi) = 0$ would hold, contrary to the fact that $G(x) = 0$ and $g(x) = 0$ are polynomial equations over $\mathbb{Q}$ of least degree satisfied by ξ.

Next let $f(x) = 0$ be any polynomial equation over $\mathbb{Q}$ have ξ as a root. Applying Theorem 9.1, we get $f(x) = g(x)q(x) + r(x)$. The remainder $r(x)$ must be identically zero, for otherwise the degree of $r(x)$ would be less than that of $g(x)$, and ξ would be a root of $r(x)$ since $f(\xi) = g(\xi) = 0$. Hence $g(x)$ is a divisor of $f(x)$.

Finally, to prove that $g(x)$ is unique, suppose that $g_1(x)$ is an irreducible monic polynomial such that $g_1(\xi) = 0$. Then $g(x) | g_1(x)$ by the argument above, say $g_1(x) = g(x)q(x)$. But the irreducibility of $g_1(x)$ then implies that $q(x)$ is a constant, in fact $q(x) = 1$ since $g_1(x)$ and $g(x)$ are monic. Thus we have $g_1(x) = g(x)$.

Definition 9.5 *The* minimal equation *of an algebraic number ξ is the equation $g(x) = 0$ described in Theorem* 9.8. *The minimal polynomial of ξ is $g(x)$. The degree of an algebraic number is the degree of its minimal polynomial.*

Definition 9.6 *An algebraic number ξ is an* algebraic integer *if it satisfies some monic polynomial equation*

$$f(x) = x^n + b_1x^{n-1} + \cdots + b_n = 0 \tag{9.3}$$

with integral coefficients.

Theorem 9.9 *Among the rational numbers, the only ones that are algebraic integers are the integers* $0, \pm 1, \pm 2, \cdots$.

Proof Any integer m is an algebraic integer because $f(x)$ can be taken as $x - m$. On the other hand, if any rational number m/q is an algebraic

integer, then we may suppose $(m, q) = 1$, and we have

$$\left(\frac{m}{q}\right)^n + b_1\left(\frac{m}{q}\right)^{n-1} + \cdots + b_n = 0,$$

$$m^n + b_1 q m^{n-1} + \cdots + b_n q^n = 0.$$

Thus $q | m^n$, so that $q = \pm 1$, and m/q is an integer.

The work "integer" in Definition 9.6 is thus simply a generalization of our previous usage. In algebraic number theory, $0, \pm 1, \pm 2, \cdots$ are often referred to as "rational integers" to distinguish them from the other algebraic integers that are not rational. For example, $\sqrt{2}$ is an algebraic integer but not a rational integer.

Theorem 9.10 *The minimal equation of an algebraic integer is monic with integral coefficients.*

Proof The equation is monic by definition, so we need prove only that the coefficients are integers. Let the algebraic integer ξ satisfy $f(x) = 0$ as in (9.3), and let its minimal equation be $g(x) = 0$, monic and irreducible over $\mathbb{Q}$. By Theorem 9.8, $g(x)$ is a divisor of $f(x)$, say $f(x) = g(x)h(x)$, and the quotient $h(x)$, like $f(x)$ and $g(x)$, is monic and has coefficients in $\mathbb{Q}$. Applying Theorem 9.7, we see that $g(x)$ has integral coefficients.

Theorem 9.11 *Let n be a positive rational integer and ξ a complex number. Suppose that the complex numbers $\theta_1, \theta_2, \cdots, \theta_n$, not all zero, satisfy the equations*

$$\xi\theta_j = a_{j,1}\theta_1 + a_{j,2}\theta_2 + \cdots + a_{j,n}\theta_n, \qquad j = 1, 2, \cdots, n \tag{9.4}$$

where the n^2 coefficients $a_{j,i}$ are rational. Then ξ is an algebraic number. Moreover, if the $a_{j,i}$ are rational integers, ξ is an algebraic integer.

Proof Equations (9.4) can be thought of as a system of homogeneous linear equations in $\theta_1, \theta_2, \cdots, \theta_n$. Since the θ_i are not all zero, the determinant of coefficients must vanish:

$$\begin{vmatrix} \xi - a_{1,1} & -a_{1,2} & \cdots & -a_{1,n} \\ -a_{2,1} & \xi - a_{2,2} & \cdots & -a_{2,n} \\ \cdots & \cdots & \cdots & \cdots \\ -a_{n,1} & -a_{n,2} & \cdots & \xi - a_{n,n} \end{vmatrix} = 0.$$

Expansion of this determinant gives an equation $\xi^n + b_1\xi^{n-1} + \cdots + b_n$

$= 0$, where the b_i are polynomials in the $a_{j,k}$. Thus the b_i are rational, and they are rational integers if the $a_{j,k}$ are.

Theorem 9.12 *If α and β are algebraic numbers, so are $\alpha + \beta$ and $\alpha\beta$. If α and β are algebraic integers, so are $\alpha + \beta$ and $\alpha\beta$.*

Proof Suppose that α and β satisfy

$$\alpha^m + a_1\alpha^{m-1} + \cdots + a_m = 0$$

$$\beta^r + b_1\beta^{r-1} + \cdots + b_r = 0$$

with rational coefficients a_i and b_j. Let $n = mr$, and define the complex numbers $\theta_1, \cdots, \theta_n$ as the numbers

$$\begin{array}{ccccc} 1, & \alpha, & \alpha^2, & \cdots, & \alpha^{m-1}, \\ \beta, & \alpha\beta, & \alpha^2\beta, & \cdots, & \alpha^{m-1}\beta, \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \beta^{r-1}, & \alpha\beta^{r-1}, & \alpha^2\beta^{r-1}, & \cdots, & \alpha^{m-1}\beta^{r-1} \end{array}$$

in any order. Thus $\theta_1, \cdots, \theta_n$ are the numbers $\alpha^s\beta^t$ with $s = 0, 1, \cdots, m-1$ and $t = 0, 1, \cdots, r-1$. Hence for any θ_j,

$$\alpha\theta_j = \alpha^{s+1}\beta^t = \begin{cases} \text{some } \theta_k & \text{if} \quad s+1 \leqslant m-1 \\ \left(-a_1\alpha^{m-1} - a_2\alpha^{m-2} - \cdots - a_m\right)\beta^t & \text{if} \quad s+1 = m \end{cases}$$

In either case we see that there are rational constants $h_{j,1}, \cdots, h_{j,n}$ such that $\alpha\theta_j = h_{j,1}\theta_1 + \cdots + h_{j,n}\theta_n$. Similarly there are rational constants $k_{j,1}, \cdots, k_{j,n}$ such that $\beta\theta_j = k_{j,1}\theta_1 + \cdots + k_{j,n}\theta_n$, and hence $(\alpha + \beta)\theta_j = (h_{j,1} + k_{j,1})\theta_1 + \cdots + (h_{j,n} + k_{j,n})\theta_n$. These equations are of the form (9.4), so we conclude that $\alpha + \beta$ is algebraic. Furthermore, if α and β are algebraic integers, then the a_j, b_j, $h_{j,i}$, $k_{j,i}$ are all rational integers, and $\alpha + \beta$ is an algebraic integer.

We also have $\alpha\beta\theta_j = \alpha(k_{j,1}\theta_1 + \cdots + k_{j,n}\theta_n) = k_{j,1}\alpha\theta_1 + \cdots + k_{j,n}\alpha\theta_n$ from which we find $\alpha\beta\theta_j = c_{j,1}\theta_1 + \cdots + c_{j,1}\theta_n$ where $c_{j,i} = k_{j,1}h_{1,i} + k_{j,2}h_{2,i} + \cdots + k_{j,n}h_{n,i}$. Again we apply Theorem 9.11 to conclude that $\alpha\beta$ is algebraic, and that it is an algebraic integer if α and β are.

This theorem states that the set of algebraic numbers is closed under addition and multiplication, and likewise for the set of algebraic integers. The following result states a little more.

Theorem 9.13 *The set of all algebraic numbers forms a field. The set of all algebraic integers forms a ring.*

Proof Rings and fields are defined in Definition 2.12. The rational numbers 0 and 1 serve as the zero and unit for the system. Most of the postulates are easily seen to be satisfied if we remember that algebraic numbers are complex numbers, whose properties we are familiar with. The only place where any difficulty arises is in proving the existence of additive and multiplicative inverses. If $\alpha \neq 0$ is a solution of

$$a_0x^n + a_1x^{n-1} + \cdots + a_n = 0$$

then $-\alpha$ and α^{-1} are solutions of

$$a_0x^n - a_1x^{n-1} + a_2x^{n-2} - \cdots + (-1)^n a_n = 0$$

and

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n = 0$$

respectively. Therefore, if α is an algebraic number, then so are $-\alpha$ and α^{-1}. If α is an algebraic integer, then so is $-\alpha$, but not necessarily α^{-1}. Therefore the algebraic numbers form a field, the algebraic integers a ring.

Example of a Transcendental Number To demonstrate that not all real numbers are algebraic, we prove that the number

$$\beta = \sum_{j=1}^{\infty} 10^{-j!} = 0.110001000\cdots$$

is trancendental. (This was one of the numbers used by Liouville in 1851 in the first proof of the existence of transcendental numbers.) Suppose β is algebraic, so that it satisfies some equation

$$f(x) = \sum_{j=0}^{n} c_j x^j = 0$$

with integral coefficients. For any x satisfying $0 < x < 1$, we have by the triangle inequality

$$|f'(x)| = \left| \sum_{j=1}^{n} jc_j x^{j-1} \right| < \sum |jc_j| = C,$$

where the constant C, defined by the last equation, depends only on the coefficients of $f(x)$. Define $\beta_k = \sum_{j=1}^{k} 10^{-j!}$ so that

$$\beta - \beta_k = \sum_{j=k+1}^{\infty} 10^{-j!} < 2 \cdot 10^{-(k+1)!}.$$

By the mean value theorem,

$$|f(\beta) - f(\beta_k)| = |\beta - \beta_k| \cdot |f'(\theta)|$$

for some θ between β and β_k. We get a contradiction by proving that the right side is smaller than the left, if k is chosen sufficiently large. The right side is smaller than $2C/10^{(k+1)!}$. Since $f(x)$ has only n zeros, we can choose k sufficiently large so that $f(\beta_k) \neq 0$. Using $f(\beta) = 0$ we see that

$$|f(\beta) - f(\beta_k)| = |f(\beta_k)| = \left| \sum_{j=0}^{n} c_j \beta_k^j \right| \geqslant 1/10^{n \cdot k!},$$

because $c_j \beta_k^j$ is a rational number with denominator $10^{j \cdot k!}$. Finally we observe that $1/10^{n \cdot k!} > 2C/10^{(k+1)!}$ if k is sufficiently large.

PROBLEMS

1. Find the minimal polynomial of each of the following algebraic numbers: 7, $\sqrt[3]{7}$, $(1 + \sqrt[3]{7})/2$, $1 + \sqrt{2} + \sqrt{3}$. Which of these are algebraic integers?
2. Prove that if α is algebraic of degree n, then $-\alpha$, α^{-1}, and $\alpha - 1$ are also of degree n, assuming $\alpha \neq 0$ in the case of α^{-1}.
3. Prove that if α is algebraic of degree n, and β is algebraic of degree m, then $\alpha + \beta$ is of degree $\leqslant mn$. Prove a similar result for $\alpha\beta$.
4. Prove that the set of real algebraic numbers (i.e., algebraic numbers that are real) forms a field, and the set of all real algebraic integers forms a ring.

9.3 ALGEBRAIC NUMBER FIELDS

The field discussed in Theorem 9.13 contains the totality of algebraic numbers. In general, an *algebraic number field* is any subset of this total collection that is a field itself. For example, if ξ is an algebraic number, then it can be readily verified that the collection of all numbers of the form $f(\xi)/h(\xi)$, $h(\xi) \neq 0$, f and h polynomials over $\mathbb{Q}$, constitutes a field. This field is denoted by $\mathbb{Q}(\xi)$, and it is called the *extension* of $\mathbb{Q}$ by ξ.

(Some authors prefer a more restrictive definition of algebraic number field than the one just given. Without going into technical details here, suffice it to say that, in effect, the restriction imposed puts an upper bound on the degrees of the algebraic numbers in the field.)