# APPENDIX 1

# The Transcendence of $e$ and $\pi$

The proof which we shall give here follows the classical method of Gelfond and Schneider, properly formulated. It is based on a theorem concerning values of functions satisfying differential equations, and it had been recognized for some time that such values are subject to severe restrictions, in various contexts. Here, we deal with the most general algebraic differential equation.

We shall assume that the reader is acquainted with elementary facts concerning functions of a complex variable. Let $f$ be an entire function (i.e. a function which is holomorphic on the complex plane). For our purposes, we say $f$ is of order $\leqq \rho$ if there exists a number $C > 1$ such that for all large $R$ we have

$$|f(z)| \leqq C^{R^\rho}$$

whenever $|z| \leqq R$. A meromorphic function is said to be of order $\leqq \rho$ if it is a quotient of entire functions of order $\leqq \rho$.

**Theorem.** *Let $K$ be a finite extension of the rational numbers. Let $f_1, \ldots, f_N$ be meromorphic functions of order $\leqq \rho$. Assume that the field $K(f_1, \ldots, f_N)$ has transcendence degree $\geqq 2$ over $K$, and that the derivative $D = d/dz$ maps the ring $K[f_1, \ldots, f_N]$ into itself. Let $w_1, \ldots, w_m$ be distinct complex numbers not lying among the poles of the $f_i$, such that*

$$f_i(w_\nu) \in K$$

*for all $i = 1, \ldots, N$ and $\nu = 1, \ldots, m$. Then $m \leqq 10\rho[K : \mathbf{Q}]$.*

**Corollary 1.** (Hermite-Lindemann). *If $\alpha$ is algebraic (over $\mathbf{Q}$) and $\neq 0$, then $e^\alpha$ is transcendental. Hence $\pi$ is transcendental.*

*Proof.* Suppose that $\alpha$ and $e^{\alpha}$ are algebraic. Let $K = \mathbf{Q}(\alpha, e^{\alpha})$. The two functions $z$ and $e^{z}$ are algebraically independent over $K$ (trivial), and the ring $K[z, e^{z}]$ is obviously mapped into itself by the derivative. Our functions take on algebraic values in $K$ at $\alpha, 2\alpha, \ldots, m\alpha$ for any $m$, contradiction. Since $e^{2\pi i} = 1$, it follows that $2\pi i$ is transcendental.

**Corollary 2.** (Gelfond-Schneider). *If $\alpha$ is algebraic $\neq 0, 1$ and if $\beta$ is algebraic irrational, then $\alpha^{\beta} = e^{\beta \log \alpha}$ is transcendental.*

*Proof.* We proceed as in Corollary 1, considering the functions $e^{\beta t}$ and $e^{t}$ which are algebraically independent because $\beta$ is assumed irrational. We look at the numbers $\log \alpha, 2 \log \alpha, \ldots, m \log \alpha$ to get a contradiction as in Corollary 1.

Before giving the main arguments proving the theorem, we state some lemmas. The first two, due to Siegel, have to do with integral solutions of linear homogeneous equations.

**Lemma 1.** *Let*

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &= 0 \\ &\cdots \\ a_{r1}x_1 + \cdots + a_{rn}x_n &= 0 \end{aligned}$$

*be a system of linear equations with integer coefficients $a_{ij}$, and $n > r$. Let $A$ be a number such that $|a_{ij}| \leqq A$ for all $i, j$. Then there exists an integral, non-trivial solution with*

$$|x_j| \leqq 2(2nA)^{r/(n-r)}.$$

*Proof.* We view our system of linear equations as a linear equation $L(X) = 0$, where $L$ is a linear map, $L : \mathbf{Z}^{(n)} \to \mathbf{Z}^{(r)}$, determined by the matrix of coefficients. If $B$ is a positive number, we denote by $\mathbf{Z}^{(n)}(B)$ the set of vectors $X$ in $\mathbf{Z}^{(n)}$ such that $|X| \leqq B$ (where $|X|$ is the maximum of the absolute values of the coefficients of $X$). Then $L$ maps $\mathbf{Z}^{(n)}(B)$ into $\mathbf{Z}^{(r)}(nBA)$. The number of elements in $\mathbf{Z}^{(n)}(B)$ is $\geqq B^n$ and $\leqq (2B + 1)^n$. We seek a value of $B$ such that there will be two distinct elements $X$, $Y$ in $\mathbf{Z}^{(n)}(B)$ having the same image, $L(X) = L(Y)$. For this, it will suffice that $B^n > (2nBA)^r$, and thus it will suffice that

$$B = (2nA)^{r/(n-r)}.$$

We take $X - Y$ as the solution of our problem.

Let $K$ be a finite extension of $\mathbf{Q}$, and let $I_K$ be the integral closure of $\mathbf{Z}$ in $K$. From Exercise 5 of Chapter IX, we know that $I_K$ is a free module over $\mathbf{Z}$, of dimension $[K : \mathbf{Q}]$. We view $K$ as contained in the complex numbers. If

$\alpha \in K$, a conjugate of $\alpha$ will be taken to be an element $\sigma\alpha$, where $\sigma$ is an embedding of $K$ in $\mathbf{C}$. By the **size** of a set of elements of $K$ we shall mean the maximum of the absolute values of all conjugates of these elements.

By the size of a vector $X = (x_1, \ldots, x_n)$ we shall mean the size of the set of its coordinates.

Let $\omega_1, \ldots, \omega_M$ be a basis of $I_K$ over $\mathbf{Z}$. Let $\alpha \in I_K$, and write

$$\alpha = a_1\omega_1 + \cdots + a_M\omega_M.$$

Let $\omega'_1, \ldots, \omega'_M$ be the dual basis of $\omega_1, \ldots, \omega_M$ with respect to the trace. Then we can express the (Fourier) coefficients $a_j$ of $\alpha$ as a trace,

$$a_j = \mathrm{Tr}(\alpha\omega'_j).$$

The trace is a sum over the conjugates. Hence the size of these coefficients is bounded by the size of $\alpha$, times a fixed constant, depending on the size of the elements $\omega'_j$.

**Lemma 2.** *Let $K$ be a finite extension of $\mathbf{Q}$. Let*

$$\begin{aligned} \alpha_{11}x_1 + \cdots + \alpha_{1n}x_n &= 0 \\ &\cdots \\ \alpha_{r1}x_1 + \cdots + \alpha_{rn}x_n &= 0 \end{aligned}$$

*be a system of linear equations with coefficients in $I_K$, and $n > r$. Let $A$ be a number such that $\mathrm{size}(\alpha_{ij}) \leqq A$, for all $i, j$. Then there exists a non-trivial solution $X$ in $I_K$ such that*

$$\mathrm{size}(X) \leqq C_1(C_2nA)^{r/(n-r)},$$

*where $C_1$, $C_2$ are constants depending only on $K$.*

*Proof.* Let $\omega_1, \ldots, \omega_M$ be a basis of $I_K$ over $\mathbf{Z}$. Each $x_j$ can be written

$$x_j = \xi_{j1}\omega_1 + \cdots + \xi_{jM}\omega_M$$

with unknowns $\xi_{j\lambda}$. Each $\alpha_{ij}$ can be written

$$\alpha_{ij} = a_{ij1}\omega_1 + \cdots + a_{ijM}\omega_M$$

with integers $a_{ij\lambda} \in \mathbf{Z}$. If we multiply out the $\alpha_{ij}x_j$, we find that our linear equations with coefficients in $I_K$ are equivalent to a system of $rM$ linear equations in the $nM$ unknowns $\xi_{j\lambda}$, with coefficients in $\mathbf{Z}$, whose size is bounded by $CA$, where $C$ is a number depending only on $M$ and the size of the elements $\omega_\lambda$, together with the products $\omega_\lambda\omega_\mu$, in other words where $C$ depends only on $K$. Applying Lemma 1, we obtain a solution in terms of the $\xi_{j\lambda}$, and hence a solution $X$ in $I_K$, whose size satisfies the desired bound.

The next lemma has to do with estimates of derivatives. By the size of a polynomial with coefficients in $K$, we shall mean the size of its set of coefficients. A **denominator** for a set of elements of $K$ will be any positive rational integer whose product with every element of the set is an algebraic integer. We define in a similar way a denominator for a polynomial with coefficients in $K$. We abbreviate "denominator" by den.

Let

$$P(T_1, \ldots, T_N) = \sum \alpha_{(\nu)} M_{(\nu)}(T)$$

be a polynomial with complex coefficients, and let

$$Q(T_1, \ldots, T_N) = \sum \beta_{(\nu)} M_{(\nu)}(T)$$

be a polynomial with real coefficients $\geqq 0$. We say that $Q$ **dominates** $P$ if $|\alpha_{(\nu)}| \leq \beta_{(\nu)}$ for all $(\nu)$. It is then immediately verified that the relation of dominance is preserved under addition, multiplication, and taking partial derivatives with respect to the variables $T_1, \ldots, T_N$.

**Lemma 3.** *Let $K$ be of finite degree over $\mathbf{Q}$. Let $f_1, \ldots, f_N$ be functions, holomorphic on a neighborhood of a point $w \in \mathbf{C}$, and assume that $D = d/dz$ maps the ring $K[f_1, \ldots, f_N]$ into itself. Assume that $f_i(w) \in K$ for all $i$. Then there exists a number $C_1$ having the following property. Let $P(T_1, \ldots, T_N)$ be a polynomial with coefficients in $K$, of degree $\leqq r$. If we set $f = P(f_1, \ldots, f_N)$, then we have, for all positive integers $k$,*

$$\text{size}(D^k f(w)) \leqq \text{size}(P) r^k k! C_1^{k+r}$$

*Furthermore, there is a denominator for $D^k f(w)$ bounded by* $\text{den}(P) C_1^{k+r}$.

*Proof.* There exist polynomials $P_i(T_1, \ldots, T_N)$ with coefficients in $K$ such that

$$Df_i = P_i(f_1, \ldots, f_N).$$

Let $h$ be the maximum of their degrees. There exists a unique derivation $\bar{D}$ on $K[T_1, \ldots, T_N]$ such that $\bar{D}T_i = P_i(T_1, \ldots, T_N)$. For any polynomial $P$ we have

$$\bar{D}(P(T_1, \ldots, T_N)) = \sum_{i=1}^{N} (D_i P)(T_1, \ldots, T_N) \cdot P_i(T_1, \ldots, T_N),$$

where $D_1, \ldots, D_N$ are the partial derivatives. The polynomial $P$ is dominated by

$$\text{size}(P)(1 + T_1 + \cdots + T_N)^r,$$

and each $P_i$ is dominated by $\text{size}(P_i)(1 + T_1 + \cdots + T_N)^h$. Thus $\bar{D}P$ is dominated by

$$\text{size}(P) C_2 r (1 + T_1 + \cdots + T_N)^{r+h}.$$

Proceeding inductively, one sees that $\bar{D}^k P$ is dominated by

$$\text{size}(P)C_3^k r^k k!(1 + T_1 \cdots + T_N)^{r+kh}.$$

Substituting values $f_i(w)$ for $T_i$, we obtain the desired bound on $D^k f(w)$. The second assertion concerning denominators is proved also by a trivial induction.

We now come to the main part of the proof of our theorem. Let $f, g$ be two functions among $f_1, \ldots, f_N$ which are algebraically independent over $K$. Let $r$ be a positive integer divisible by $2m$. We shall let $r$ tend to infinity at the end of the proof.

Let

$$F = \sum_{i,j=1}^{r} b_{ij} f^i g^j$$

have coefficients $b_{ij}$ in $K$. Let $n = r^2/2m$. We can select the $b_{ij}$ not all equal to 0, and such that

$$D^k F(w_v) = 0$$

for $0 \leqq k < n$ and $v = 1, \ldots, m$. Indeed, we have to solve a system of $mn$ linear equations in $r^2 = 2mn$ unknowns. Note that

$$\frac{mn}{2mn - mn} = 1.$$

We multiply these equations by a denominator for the coefficients. Using the estimate of Lemma 3, and Lemma 2, we can in fact take the $b_{ij}$ to be algebraic integers, whose size is bounded by

$$O(r^n n! C_1^{n+r}) \leqq O(n^{2n})$$

for $n \to \infty$.

Since $f$, $g$ are algebraically independent over $K$, our function $F$ is not identically zero. We let $s$ be the smallest integer such that all derivatives of $F$ up to order $s - 1$ vanish at all points $w_1, \ldots, w_m$, but such that $D^s F$ does not vanish at one of the $w$, say $w_1$. Then $s \geqq n$. We let

$$\gamma = D^s F(w_1) \neq 0.$$

Then $\gamma$ is an element of $K$, and by Lemma 3, it has a denominator which is bounded by $O(C_1^s)$ for $s \to \infty$. Let $c$ be this denominator. The norm of $c\gamma$ from $K$ to $\mathbf{Q}$ is then a non-zero rational integer. Each conjugate of $c\gamma$ is bounded by $O(s^{5s})$. Consequently, we get

$$1 \leqq |N_{\mathbf{Q}}^K(c\gamma)| \leqq O(s^{5s})^{[K:\mathbf{Q}]-1} |\gamma|, \tag{1}$$

where $|\gamma|$ is the fixed absolute value of $\gamma$, which will now be estimated very well by global arguments.

Let $\theta$ be an entire function of order $\leqq \rho$, such that $\theta f$ and $\theta g$ are entire, and $\theta(w_1) \neq 0$. Then $\theta^{2r}F$ is entire. We consider the entire function

$$H(z) = \frac{\theta(z)^{2r}F(z)}{\prod_{v=1}^{m}(z - w_v)^s}.$$

Then $H(w_1)$ differs from $D^sF(w_1)$ by obvious factors, bounded by $C_4^s s!$. By the maximum modulus principle, its absolute value is bounded by the maximum of $H$ on a large circle of radius $R$. If we take $R$ large, then $z - w_v$ has approximately the same absolute value as $R$, and consequently, on the circle of radius $R$, $H(z)$ is bounded in absolute value by an expression of type

$$\frac{s^{3s}C_5^{2rR^\rho}}{R^{ms}}.$$

We select $R = s^{1/2\rho}$. We then get the estimate

$$|\gamma| \leqq \frac{s^{4s}C_6^s}{s^{ms/2\rho}}.$$

We now let $r$ tend to infinity. Then both $n$ and $s$ tend to infinity. Combining this last inequality with inequality (1), we obtain the desired bound on $m$. This concludes the proof.

Of course, we made no effort to be especially careful in the powers of $s$ occurring in the estimates, and the number 10 can obviously be decreased by exercising a little more care in the estimates.

The theorem we proved is only the simplest in an extensive theory dealing with problems of transcendence degree. In some sense, the theorem is best possible without additional hypotheses. For instance, if $P(t)$ is a polynomial with integer coefficients, then $e^{P(t)}$ will take the value 1 at all roots of $P$, these being algebraic. Furthermore, the functions

$$t, e^t, e^{t^2}, \ldots, e^{t^n}$$

are algebraically independent, but take on values in $\mathbf{Q}(e)$ for all integral values of $t$.

However, one expects rather strong results of algebraic independence to hold. Lindemann proved that *if* $\alpha_1, \ldots, \alpha_n$ *are algebraic numbers, linearly independent over* $\mathbf{Q}$, *then*

$$e^{\alpha_1}, \ldots, e^{\alpha_n}$$

*are algebraically independent.*

More generally, Schanuel has made the following conjecture: If $\alpha_1, \ldots, \alpha_n$ are complex numbers, linearly independent over $\mathbf{Q}$, then the transcendence degree of

$$\alpha_1, \ldots, \alpha_n, e^{\alpha_1}, \ldots, e^{\alpha_n}$$

should be $\geqq n$.

From this one would deduce at once the algebraic independence of $e$ and $\pi$ (looking at $1, 2\pi i, e, e^{2\pi i}$), and all other independence statements concerning the ordinary exponential function and logarithm which one feels to be true, for instance, the statement that $\pi$ cannot lie in the field obtained by starting with the algebraic numbers, adjoining values of the exponential function, taking algebraic closure, and iterating these two operations. Such statements have to do with values of the exponential function lying in certain fields of transcendence degree $< n$, and one hopes that by a suitable deepening of Theorem 1, one will reach the desired results.

# APPENDIX 2

# Some Set Theory

## §1. DENUMERABLE SETS

Let $n$ be a positive integer. Let $J_n$ be the set consisting of all integers $k$, $1 \leqq k \leqq n$. If $S$ is a set, we say that $S$ has $n$ elements if there is a bijection between $S$ and $J_n$. Such a bijection associates with each integer $k$ as above an element of $S$, say $k \mapsto a_k$. Thus we may use $J_n$ to "count" $S$. Part of what we assume about the basic facts concerning positive integers is that if $S$ has $n$ elements, then the integer $n$ is uniquely determined by $S$.

One also agrees to say that a set has 0 elements if the set is empty.

We shall say that a set $S$ is **denumerable** if there exists a bijection of $S$ with the set of positive integers $\mathbf{Z}^+$. Such a bijection is then said to **enumerate** the set $S$. It is a mapping

$$n \mapsto a_n$$

which to each positive integer $n$ associates an element of $S$, the mapping being injective and surjective.

If $D$ is a denumerable set, and $f : S \to D$ is a bijection of some set $S$ with $D$, then $S$ is also denumerable. Indeed, there is a bijection $g : D \to \mathbf{Z}^+$, and hence $g \circ f$ is a bijection of $S$ with $\mathbf{Z}^+$.

Let $T$ be a set. A **sequence** of elements of $T$ is simply a mapping of $\mathbf{Z}^+$ into $T$. If the map is given by the association $n \mapsto x_n$, we also write the sequence as $\{x_n\}_{n \geqq 1}$, or also $\{x_1, x_2, \ldots\}$. For simplicity, we also write $\{x_n\}$ for the sequence. Thus we think of the sequence as prescribing a first, second, ..., $n$-th element of $T$. We use the same braces for sequences as for sets, but the context will always make our meaning clear.

**Examples.** The even positive integers may be viewed as a sequence $\{x_n\}$ if we put $x_n = 2n$ for $n = 1, 2, \ldots$. The odd positive integers may also be viewed as a sequence $\{y_n\}$ if we put $y_n = 2n - 1$ for $n = 1, 2, \ldots$. In each case, the sequence gives an enumeration of the given set.

We also use the word *sequence* for mappings of the natural numbers into a set, thus allowing our sequences to start from 0 instead of 1. If we need to specify whether a sequence starts with the 0-th term or the first term, we write

$$\{x_n\}_{n \geqq 0} \quad \text{or} \quad \{x_n\}_{n \geqq 1}$$

according to the desired case. Unless otherwise specified, however, we always assume that a sequence will start with the first term. Note that from a sequence $\{x_n\}_{n \geqq 0}$ we can define a new sequence by letting $y_n = x_{n-1}$ for $n \geqq 1$. Then $y_1 = x_0, y_2 = x_1, \ldots$. Thus there is no essential difference between the two kinds of sequences.

Given a sequence $\{x_n\}$, we call $x_n$ the $n$-th term of the sequence. A sequence may very well be such that all its terms are equal. For instance, if we let $x_n = 1$ for all $n \geqq 1$, we obtain the sequence $\{1, 1, 1, \ldots\}$. Thus there is a difference between a sequence of elements in a set $T$, and a subset of $T$. In the example just given, the set of all terms of the sequence consists of one element, namely the single number 1.

Let $\{x_1, x_2, \ldots\}$ be a sequence in a set $S$. By a **subsequence** we shall mean a sequence $\{x_{n_1}, x_{n_2}, \ldots\}$ such that $n_1 < n_2 < \cdots$. For instance, if $\{x_n\}$ is the sequence of positive integers, $x_n = n$, the sequence of even positive integers $\{x_{2n}\}$ is a subsequence.

An enumeration of a set $S$ is of course a sequence in $S$.

A set is **finite** if the set is empty, or if the set has $n$ elements for some positive integer $n$. If a set is not finite, it is called **infinite**.

Occasionally, a map of $J_n$ into a set $T$ will be called a **finite sequence** in $T$. A finite sequence is written as usual,

$$\{x_1, \ldots, x_n\} \quad \text{or} \quad \{x_i\}_{i=1,\ldots,n}.$$

When we need to specify the distinction between finite sequences and maps of $\mathbf{Z}^+$ into $T$, we call the latter infinite sequences. Unless otherwise specified, we shall use the word sequence to mean infinite sequence.

**Proposition 1.1.** *Let $D$ be an infinite subset of $\mathbf{Z}^+$. Then $D$ is denumerable, and in fact there is a unique enumeration of $D$, say $\{k_1, k_2, \ldots\}$ such that*

$$k_1 < k_2 < \cdots < k_n < k_{n+1} < \cdots.$$

*Proof.* We let $k_1$ be the smallest element of $D$. Suppose inductively that we have defined $k_1 < \cdots < k_n$, in such a way that any element $k$ in $D$ which is not equal to $k_1, \ldots, k_n$ is $> k_n$. We define $k_{n+1}$ to be the smallest element of $D$ which is $> k_n$. Then the map $n \mapsto k_n$ is the desired enumeration of $D$.

**Corollary 1.2.** *Let $S$ be a denumerable set and $D$ an infinite subset of $S$. Then $D$ is denumerable.*

*Proof.* Given an enumeration of $S$, the subset $D$ corresponds to a subset of $\mathbf{Z}^+$ in this enumeration. Using Proposition 1.1, we conclude that we can enumerate $D$.

**Proposition 1.3.** *Every infinite set contains a denumerable subset.*

*Proof.* Let $S$ be an infinite set. For every non-empty subset $T$ of $S$, we select a definite element $a_T$ in $T$. We then proceed by induction. We let $x_1$ be the chosen element $a_S$. Suppose that we have chosen $x_1, \ldots, x_n$ having the property that for each $k = 2, \ldots, n$ the element $x_k$ is the selected element in the subset which is the complement of $\{x_1, \ldots, x_{k-1}\}$. We let $x_{n+1}$ be the selected element in the complement of the set $\{x_1, \ldots, x_n\}$. By induction, we thus obtain an association $n \mapsto x_n$ for all positive integers $n$, and since $x_n \neq x_k$ for all $k < n$ it follows that our association is injective, i.e. gives an enumeration of a subset of $S$.

**Proposition 1.4.** *Let $D$ be a denumerable set, and $f : D \to S$ a surjective mapping. Then $S$ is denumerable or finite.*

*Proof.* For each $y \in S$, there exists an element $x_y \in D$ such that $f(x_y) = y$ because $f$ is surjective. The association $y \mapsto x_y$ is an injective mapping of $S$ into $D$, because if

$$y, z \in S \quad \text{and} \quad x_y = x_z$$

then

$$y = f(x_y) = f(x_z) = z.$$

Let $g(y) = x_y$. The image of $g$ is a subset of $D$ and $D$ is denumerable. Since $g$ is a bijection between $S$ and its image, it follows that $S$ is denumerable or finite.

**Proposition 1.5.** *Let $D$ be a denumerable set. Then $D \times D$ (the set of all pairs $(x, y)$ with $x, y \in D$) is denumerable.*

*Proof.* There is a bijection between $D \times D$ and $\mathbf{Z}^+ \times \mathbf{Z}^+$, so it will suffice to prove that $\mathbf{Z}^+ \times \mathbf{Z}^+$ is denumerable. Consider the mapping of $\mathbf{Z}^+ \times \mathbf{Z}^+ \to \mathbf{Z}^+$ given by

$$(m, n) \mapsto 2^n 3^m.$$

It is injective, and by Proposition 1.1, our result follows.

**Proposition 1.6.** *Let $\{D_1, D_2, \ldots\}$ be a sequence of denumerable sets. Let $S$ be the union of all sets $D_i$ $(i = 1, 2, \ldots)$. Then $S$ is denumerable.*

*Proof.* For each $i = 1, 2, \ldots$ we enumerate the elements of $D_i$, as indicated in the following notation:

$$\begin{aligned} D_1&: \{x_{11}, x_{12}, x_{13}, \ldots\} \\ D_2&: \{x_{21}, x_{22}, x_{23}, \ldots\} \\ &\cdots \\ D_i&: \{x_{i1}, x_{i2}, x_{i3}, \ldots\} \\ &\cdots \end{aligned}$$

The map $f: \mathbf{Z}^+ \times \mathbf{Z}^+ \to D$ given by

$$f(i, j) = x_{ij}$$

is then a surjective map of $\mathbf{Z}^+ \times \mathbf{Z}^+$ onto $S$. By Proposition 1.4, it follows that $S$ is denumerable.

**Corollary 1.7.** *Let $F$ be a non-empty finite set and $D$ a denumerable set. Then $F \times D$ is denumerable. If $S_1, S_2, \ldots$ are a sequence of sets, each of which is finite or denumerable, then the union $S_1 \cup S_2 \cup \cdots$ is denumerable or finite.*

*Proof.* There is an injection of $F$ into $\mathbf{Z}^+$ and a bijection of $D$ with $\mathbf{Z}^+$. Hence there is an injection of $F \times \mathbf{Z}^+$ into $\mathbf{Z}^+ \times \mathbf{Z}^+$ and we can apply Corollary 1.2 and Proposition 1.6 to prove the first statement. One could also define a surjective map of $\mathbf{Z}^+ \times \mathbf{Z}^+$ onto $F \times D$. (Cf. Exercises 1 and 4.) As for the second statement, each finite set is contained in some denumerable set, so that the second statement follows from Proposition 1.1 and 1.6.

For convenience, we shall say that a set is **countable** if it is either finite or denumerable.

## §2. ZORN'S LEMMA

In order to deal efficiently with infinitely many sets simultaneously, one needs a special property. To state it, we need some more terminology.

Let $S$ be a set. An **ordering** (also called partial ordering) of $S$ is a relation, written $x \leqq y$, among some pairs of elements of $S$, having the following properties.

**ORD 1.** *We have $x \leqq x$.*

**ORD 2.** *If $x \leqq y$ and $y \leqq z$ then $x \leqq z$.*

**ORD 3.** *If $x \leqq y$ and $y \leqq x$ then $x = y$.*

We sometimes write $y \geqq x$ for $x \leqq y$. Note that we don't require that the relation $x \leqq y$ or $y \leqq x$ hold for every pair of elements $(x, y)$ of $S$. Some pairs may not be comparable. If the ordering satisfies this additional property, then we say that it is a **total ordering**.

**Example 1.** Let $G$ be a group. Let $S$ be the set of subgroups. If $H$, $H'$ are subgroups of $G$, we define

$$H \leqq H'$$

if $H$ is a subgroup of $H'$. One verifies immediately that this relation defines an ordering on $S$. Given two subgroups $H$, $H'$ of $G$, we do not necessarily have $H \leqq H'$ or $H' \leqq H$.

**Example 2.** Let $R$ be a ring, and let $S$ be the set of left ideals of $R$. We define an ordering in $S$ in a way similar to the above, namely if $L$, $L'$ are left ideals of $R$, we define

$$L \leqq L'$$

if $L \subset L'$.

**Example 3.** Let $X$ be a set, and $S$ the set of subsets of $X$. If $Y, Z$ are subsets of $X$, we define $Y \leqq Z$ if $Y$ is a subset of $Z$. This defines an ordering on $S$.

In all these examples, the relation of ordering is said to be that of inclusion.

In an ordered set, if $x \leqq y$ and $x \neq y$ we then write $x < y$.

Let $A$ be an ordered set, and $B$ a subset. Then we can define an ordering on $B$ by defining $x \leqq y$ for $x, y \in B$ to hold if and only if $x \leqq y$ in $A$. We shall say that $R_0$ is the ordering on $B$ **induced** by $R$, or is the **restriction** to $B$ of the partial ordering of $A$.

Let $S$ be an ordered set. By a **least** element of $S$ (or a **smallest** element) one means an element $a \in S$ such that $a \leqq x$ for all $x \in S$. Similarly, by a **greatest element** one means an element $b$ such that $x \leqq b$ for all $x \in S$.

By a **maximal element** $m$ of $S$ one means an element such that if $x \in S$ and $x \geqq m$, then $x = m$. Note that a maximal element need not be a greatest element. There may be many maximal elements in $S$, whereas if a greatest element exists, then it is unique (proof ?).

Let $S$ be an ordered set. We shall say that $S$ is **totally ordered** if given $x, y \in S$ we have necessarily $x \leqq y$ or $y \leqq x$.

**Example 4.** The integers $\mathbf{Z}$ are totally ordered by the usual ordering. So are the real numbers.

Let $S$ be an ordered set, and $T$ a subset. An **upper bound** of $T$ (in $S$) is an element $b \in S$ such that $x \leqq b$ for all $x \in T$. A **least upper bound** of $T$ in $S$ is an upper bound $b$ such that, if $c$ is another upper bound, then $b \leqq c$. We shall say

that $S$ is **inductively ordered** if every non-empty totally ordered subset has an upper bound.

We shall say that $S$ is **strictly** inductively ordered if every non-empty totally ordered subset has a least upper bound.

In Examples 1, 2, 3, in each case, the set is strictly inductively ordered. To prove this, let us take Example 1. Let $T$ be a non-empty totally ordered subset of the set of subgroups of $G$. This means that if $H, H' \in T$, then $H \subset H'$ or $H' \subset H$. Let $U$ be the union of all sets in $T$. Then:

1. $U$ is a subgroup. *Proof*: If $x, y \in U$, there exist subgroups $H, H' \in T$ such that $x \in H$ and $y \in H'$. If, say, $H \subset H'$, then both $x, y \in H'$ and hence $xy \in H'$. Hence $xy \in U$. Also, $x^{-1} \in H'$, so $x^{-1} \in U$. Hence $U$ is a subgroup.
2. $U$ is an upper bound for each element of $T$. *Proof*: Every $H \in T$ is contained in $U$, so $H \leqq U$ for all $H \in T$.
3. $U$ is a least upper bound for $T$. *Proof*: Any subgroup of $G$ which contains all the subgroups $H \in T$ must then contain their union $U$.

The proof that the sets in Examples 2, 3 are strictly inductively ordered is entirely similar.

We can now state the property mentioned at the beginning of the section.

**Zorn's Lemma.** *Let $S$ be a non-empty inductively ordered set. Then there exists a maximal element in $S$.*

As an example of Zorn's lemma, we shall now prove the infinite version of a theorem given in Chapters 1, §7, and XIV, §2, namely:

*Let $R$ be an entire, principal ring and let $E$ be a free module over $R$. Let $F$ be a submodule. Then $F$ is free. In fact, if $\{v_i\}_{i \in I}$ is a basis for $E$, and $F \neq \{0\}$, then there exists a basis for $F$ indexed by a subset of $I$.*

*Proof.* For each subset $J$ of $I$ we let $E_J$ be the free submodule of $E$ generated by all $v_j, j \in J$, and we let $F_J = E_J \cap F$. We let $S$ be the set of all pairs $(F_J, w)$ where $J$ is a subset of $I$, and $w : J' \to F_J$ is a basis of $F_J$ indexed by a subset $J'$ of $J$. We write $w_j$ instead of $w(j)$ for $j \in J'$. If $(F_J, w)$ and $(F_K, u)$ are such pairs, we define $(F_J, w) \leqq (F_K, u)$ if $J \subset K$, if $J' \subset K'$, and if the restriction of $u$ to $J'$ is equal to $w$. (In other words, the basis $u$ for $F_K$ is an extension of the basis $w$ for $F_J$.) This defines an ordering on $S$, and it is immediately verified that $S$ is in fact inductively ordered, and non-empty (say by the finite case of the result). We can therefore apply Zorn's lemma. Let $(F_J, w)$ be a maximal element. We contend that $J = I$ (this will prove our result). Suppose $J \neq I$ and let $k \in I$ but $k \notin J$. Let $K = J \cup \{k\}$. If

$$E_{J \cup \{k\}} \cap F = F_J,$$

then $(F_K, w)$ is a bigger pair than $(F_J, w)$ contradicting the maximality assumption. Qtherwise there exist elements of $F_K$ which can be written in the form

$$cv_k + y$$

with some $y \in E_J$ and $c \in R$, $c \neq 0$. The set of all elements $c \in R$ such that there exists $y \in E_J$ for which $cv_k + y \in F$ is an ideal. Let $a$ be a generator of this ideal, and let

$$w_k = av_k + y$$

be an element of $F$, with $y \in E_J$. If $z \in F_K$ then there exists $b \in R$ such that $z - bw_k \in E_J$. But $z - bw_k \in F$, whence $z - bw_k \in F_J$. It follows at once that the family consisting of $w_j$ $(j \in J)$ and $w_k$ is a basis for $F_K$, thus contradicting the maximality again. This proves what we wanted.

Zorn's lemma could be just taken as an axiom of set theory. However, it is not psychologically completely satisfactory as an axiom, because its statement is too involved, and one does not visualize easily the existence of the maximal element asserted in that statement. We show how one can prove Zorn's lemma from other properties of sets which everyone would immediately grant as acceptable psychologically.

From now on to the end of the proof of Theorem 2.1, we let $A$ be a non-empty partially ordered and strictly inductively ordered set. We recall that **strictly inductively ordered** means that every nonempty totally ordered subset has a least upper bound. We assume given a map $f : A \to A$ such that for all $x \in A$ we have $x \leqq f(x)$. We could call such a map an **increasing** map.

Let $a \in A$. Let $B$ be a subset of $A$. We shall say that $B$ is **admissible** if:

1. $B$ contains $a$.
2. We have $f(B) \subset B$.
3. Whenever $T$ is a non-empty totally ordered subset of $B$, the least upper bound of $T$ in $A$ lies in $B$.

Then $B$ is also strictly inductively ordered, by the induced ordering of $A$. We shall prove:

**Theorem 2.1.** (Bourbaki). *Let $A$ be a non-empty partially ordered and strictly inductively ordered set. Let $f : A \to A$ be an increasing mapping. Then there exists an element $x_0 \in A$ such that $f(x_0) = x_0$.*

*Proof.* Suppose that $A$ were totally ordered. By assumption, it would have a least upper bound $b \in A$, and then

$$b \leqq f(b) \leqq b,$$

so that in this case, our theorem is clear. The whole problem is to reduce the theorem to that case. In other words, what we need to find is a totally ordered admissible subset of $A$.

If we throw out of $A$ all elements $x \in A$ such that $x$ is not $\geqq a$, then what remains is obviously an admissible subset. Thus without loss of generality, we may assume that $A$ has a least element $a$, that is $a \leqq x$ for all $x \in A$.

Let $M$ be the intersection of all admissible subsets of $A$. Note that $A$ itself is an admissible subset, and that all admissible subsets of $A$ contain $a$, so that $M$ is not empty. Furthermore, $M$ is itself an admissible subset of $A$. To see this, let $x \in M$. Then $x$ is in every admissible subset, so $f(x)$ is also in every admissible subset, and hence $f(x) \in M$. Hence $f(M) \subset M$. If $T$ is a totally ordered non-empty subset of $M$, and $b$ is the least upper bound of $T$ in $A$, then $b$ lies in every admissible subset of $A$, and hence lies in $M$. It follows that $M$ is the smallest admissible subset of $A$, and that any admissible subset of $A$ contained in $M$ is equal to $M$.

We shall prove that $M$ is totally ordered, and thereby prove Theorem 2.1.

[First we make some remarks which don't belong to the proof, but will help in the understanding of the subsequent lemmas. Since $a \in M$, we see that $f(a) \in M$, $f \circ f(a) \in M$, and in general $f^n(a) \in M$. Furthermore,

$$a \leqq f(a) \leqq f^2(a) \leqq \cdots.$$

If we had an equality somewhere, we would be finished, so we may assume that the inequalities hold. Let $D_0$ be the totally ordered set $\{f^n(a)\}_{n \geqq 0}$. Then $D_0$ looks like this:

$$a < f(a) < f^2(a) < \cdots < f^n(a) < \cdots.$$

Let $a_1$ be the least upper bound of $D_0$. Then we can form

$$a_1 < f(a_1) < f^2(a_1) < \cdots$$

in the same way to obtain $D_1$, and we can continue this process, to obtain

$$D_1, D_2, \ldots.$$

It is clear that $D_1, D_2, \ldots$ are contained in $M$. If we had a precise way of expressing the fact that we can establish a never-ending string of such denumerable sets, then we would obtain what we want. The point is that we are now trying to prove Zorn's lemma, which is the natural tool for guaranteeing the existence of such a string. However, given such a string, we observe that its elements have two properties: If $c$ is an element of such a string and $x < c$, then $f(x) \leqq c$. Furthermore, there is no element between $c$ and $f(c)$, that is if $x$ is an element of the string, then $x \leqq c$ or $f(c) \leqq x$. We shall now prove two lemmas which show that elements of $M$ have these properties.]

Let $c \in M$. We shall say that $c$ is an **extreme point** of $M$ if whenever $x \in M$ and $x < c$, then $f(x) \leqq c$. For each extreme point $c \in M$ we let

$$M_c = \text{set of } x \in M \quad \text{such that} \quad x \leqq c \quad \text{or} \quad f(c) \leqq x.$$

Note that $M_c$ is not empty because $a$ is in it.

**Lemma 2.2.** *We have $M_c = M$ for every extreme point $c$ of $M$.*

*Proof.* It will suffice to prove that $M_c$ is an admissible subset. Let $x \in M_c$. If $x < c$ then $f(x) \leqq c$ so $f(x) \in M_c$. If $x = c$ then $f(x) = f(c)$ is again in $M_c$. If $f(c) \leqq x$, then $f(c) \leqq x \leqq f(x)$, so once more $f(x) \in M_c$. Thus we have proved that $f(M_c) \subset M_c$.

Let $T$ be a totally ordered subset of $M_c$ and let $b$ be the least upper bound of $T$ in $M$. If all elements $x \in T$ are $\leqq c$, then $b \leqq c$ and $b \in M_c$. If some $x \in T$ is such that $f(c) \leqq x$, then $f(c) \leqq x \leqq b$, and so $b$ is in $M_c$. This proves our lemma.

**Lemma 2.3.** *Every element of $M$ is an extreme point.*

*Proof.* Let $E$ be the set of extreme points of $M$. Then $E$ is not empty because $a \in E$. It will suffice to prove that $E$ is an admissible subset. We first prove that $f$ maps $E$ into itself. Let $c \in E$. Let $x \in M$ and suppose $x < f(c)$. We must prove that $f(x) \leqq f(c)$. By Lemma 2.2, $M = M_c$, and hence we have $x < c$, or $x = c$, or $f(c) \leqq x$. This last possibility cannot occur because $x < f(c)$. If $x < c$ then

$$f(x) \leqq c \leqq f(c).$$

If $x = c$ then $f(x) = f(c)$, and hence $f(E) \subset E$.

Next let $T$ be a totally ordered subset of $E$. Let $b$ be the least upper bound of $T$ in $M$. We must prove that $b \in E$. Let $x \in M$ and $x < b$. If for all $c \in T$ we have $f(c) \leqq x$, then $c \leqq f(c) \leqq x$ implies that $x$ is an upper bound for $T$, whence $b \leqq x$, which is impossible. Since $M_c = M$ for all $c \in E$, we must therefore have $x \leqq c$ for some $c \in T$. If $x < c$, then $f(x) \leqq c \leqq b$, and if $x = c$, then

$$c = x < b.$$

Since $c$ is an extreme point and $M_c = M$, we get $f(x) \leqq b$. This proves that $b \in E$, that $E$ is admissible, and thus proves Lemma 2.3.

We now see trivially that $M$ is totally ordered. For let $x, y \in M$. Then $x$ is an extreme point of $M$ by Lemma 2, and $y \in M_x$ so $y \leqq x$ or

$$x \leqq f(x) \leqq y,$$

thereby proving that $M$ is totally ordered. As remarked previously, this concludes the proof of Theorem 2.1.

We shall obtain Zorn's lemma essentially as a corollary of Theorem 2.1. We first obtain Zorn's lemma in a slightly weaker form.

**Corollary 2.4.** *Let $A$ be a non-empty strictly inductively ordered set. Then $A$ has a maximal element.*

*Proof.* Suppose that $A$ does not have a maximal element. Then for each $x \in A$ there exists an element $y_x \in A$ such that $x < y_x$. Let $f: A \to A$ be the map such that $f(x) = y_x$ for all $x \in A$. Then $A, f$ satisfy the hypotheses of Theorem 2.1 and applying Theorem 2.1 yields a contradiction.

The only difference between Corollary 2.4 and Zorn's lemma is that in Corollary 2.4, we assume that a non-empty totally ordered subset has a *least* upper bound, rather than an upper bound. It is, however, a simple matter to reduce Zorn's lemma to the seemingly weaker form of Corollary 2.4. We do this in the second corollary.

**Corollary 2.5. (Zorn's lemma).** *Let $S$ be a non-empty inductively ordered set. Then $S$ has a maximal element.*

*Proof.* Let $A$ be the set of non-empty totally ordered subsets of $S$. Then $A$ is not empty since any subset of $S$ with one element belongs to $A$. If $X, Y \in A$, we define $X \leqq Y$ to mean $X \subset Y$. Then $A$ is partially ordered, and is in fact strictly inductively ordered. For let $T = \{X_i\}_{i \in I}$ be a totally ordered subset of $A$. Let

$$Z = \bigcup_{i \in I} X_i.$$

Then $Z$ is totally ordered. To see this, let $x, y \in Z$. Then $x \in X_i$ and $y \in X_j$ for some $i, j \in I$. Since $T$ is totally ordered, say $X_i \subset X_j$. Then $x, y \in X_j$ and since $X_j$ is totally ordered, $x \leqq y$ or $y \leqq x$. Thus $Z$ is totally ordered, and is obviously a least upper bound for $T$ in $A$. By Corollary 2.4, we conclude that $A$ has a maximal element $X_0$. This means that $X_0$ is a maximal totally ordered subset of $S$ (non-empty). Let $m$ be an upper bound for $X_0$ in $S$. Then $m$ is the desired maximal element of $S$. For if $x \in S$ and $m \leqq x$ then $X_0 \cup \{x\}$ is totally ordered, whence equal to $X_0$ by the maximality of $X_0$. Thus $x \in X_0$ and $x \leqq m$. Hence $x = m$, as was to be shown.

## §3. CARDINAL NUMBERS

Let $A$, $B$ be sets. We shall say that the **cardinality** *of $A$ is the same as the cardinality of $B$*, and write

$$\text{card}(A) = \text{card}(B)$$

if there exists a bijection of $A$ onto $B$.

We say $\text{card}(A) \leqq \text{card}(B)$ if there exists an injective mapping (injection) $f: A \to B$. We also write $\text{card}(B) \geqq \text{card}(A)$ in this case. It is clear that if $\text{card}(A) \leqq \text{card}(B)$ and $\text{card}(B) \leqq \text{card}(C)$, then $\text{card}(A) \leqq \text{card}(C)$.

This amounts to saying that a composite of injective mappings is injective. Similarly, if $\text{card}(A) = \text{card}(B)$ and $\text{card}(B) = \text{card}(C)$ then $\text{card}(A) = \text{card}(C)$.

This amounts to saying that a composite of bijective mappings is bijective. We clearly have $\text{card}(A) = \text{card}(A)$. Using Zorn's lemma, it is easy to show (see Exercise 14) that

$$\text{card}(A) \leqq \text{card}(B) \quad \text{or} \quad \text{card}(B) \leqq \text{card}(A).$$

*Let $f: A \to B$ be a surjective map of a set $A$ onto a set $B$. Then*

$$\text{card}(B) \leqq \text{card}(A).$$

This is easily seen, because for each $y \in B$ there exists an element $x \in A$, denoted by $x_y$, such that $f(x_y) = y$. Then the association $y \mapsto x_y$ is an injective mapping of $B$ into $A$, whence by definition, $\text{card}(B) \leqq \text{card}(A)$.

*Given two nonempty sets $A$, $B$ we have* $\text{card}(A) \leqq \text{card}(B)$ *or* $\text{card}(B) \leqq \text{card}(A)$.

This is a simple application of Zorn's lemma. We consider the family of pairs $(S, f)$ where $S$ is a subset of $A$ and $f: S \to B$ is an injective mapping. From the existence of a maximal element, the assertion follows at once.

**Theorem 3.1.** (Schroeder-Bernstein). *Let $A$, $B$ be sets, and suppose that* $\text{card}(A) \leqq \text{card}(B)$, *and* $\text{card}(B) \leqq \text{card}(A)$. *Then*

$$\text{card}(A) = \text{card}(B).$$

*Proof.* Let

$$f: A \to B \quad \text{and} \quad g: B \to A$$

be injections. We separate $A$ into two disjoint sets $A_1$ and $A_2$. We let $A_1$ consist of all $x \in A$ such that, when we lift back $x$ by a succession of inverse maps,

$$x, \ g^{-1}(x), \quad f^{-1} \circ g^{-1}(x), \quad g^{-1} \circ f^{-1} \circ g^{-1}(x), \ldots$$

then at some stage we reach an element of $A$ which cannot be lifted back to $B$ by $g$. We let $A_2$ be the complement of $A_1$, in other words, the set of $x \in A$ which can be lifted back indefinitely, or such that we get stopped in $B$ (i.e. reach an element of $B$ which has no inverse image in $A$ by $f$). Then $A = A_1 \cup A_2$. We shall define a bijection $h$ of $A$ onto $B$.

If $x \in A_1$, we define $h(x) = f(x)$.

If $x \in A_2$, we define $h(x) = g^{-1}(x) =$ unique element $y \in B$ such that $g(y) = x$.

Then trivially, $h$ is injective. We must prove that $h$ is surjective. Let $b \in B$. If, when we try to lift back $b$ by a succession of maps

$$\cdots \circ f^{-1} \circ g^{-1} \circ f^{-1} \circ g^{-1} \circ f^{-1}(b)$$

we can lift back indefinitely, or if we get stopped in $B$, then $g(b)$ belongs to $A_2$ and consequently $b = h(g(b))$, so $b$ lies in the image of $h$. On the other hand, if we cannot lift back $b$ indefinitely, and get stopped in $A$, then $f^{-1}(b)$ is defined (i.e., $b$ is in the image of $f$), and $f^{-1}(b)$ lies in $A_1$. In this case, $b = h(f^{-1}(b))$ is also in the image of $h$, as was to be shown.

Next we consider theorems concerning sums and products of cardinalities.

We shall reduce the study of cardinalities of products of arbitrary sets to the denumerable case, using Zorn's lemma. Note first that an infinite set $A$ always contains a denumerable set. Indeed, since $A$ is infinite, we can first select an element $a_1 \in A$, and the complement of $\{a_1\}$ is infinite. Inductively, if we have selected distinct elements $a_1, \ldots, a_n$ in $A$, the complement of $\{a_1, \ldots, a_n\}$ is infinite, and we can select $a_{n+1}$ in this complement. In this way, we obtain a sequence of distinct elements of $A$, giving rise to a denumerable subset of $A$.

Let $A$ be a set. By a **covering** of $A$ one means a set $\Gamma$ of subsets of $A$ such that the union

$$\bigcup_{C \in \Gamma} C$$

of all the elements of $\Gamma$ is equal to $A$. We shall say that $\Gamma$ is a **disjoint covering** if whenever $C, C' \in \Gamma$, and $C \neq C'$, then the intersection of $C$ and $C'$ is empty.

**Lemma 3.2.** *Let $A$ be an infinite set. Then there exists a disjoint covering of $A$ by denumerable sets.*

*Proof.* Let $S$ be the set whose elements are pairs $(B, \Gamma)$ consisting of a subset $B$ of $A$, and a disjoint covering of $B$ by denumerable sets. Then $S$ is not empty. Indeed, since $A$ is infinite, $A$ contains a denumerable set $D$, and the pair $(D, \{D\})$ is in $S$. If $(B, \Gamma)$ and $(B', \Gamma')$ are elements of $S$, we define

$$(B, \Gamma) \leqq (B', \Gamma')$$

to mean that $B \subset B'$, and $\Gamma \subset \Gamma'$. Let $T$ be a totally ordered non-empty subset of $S$. We may write $T = \{(B_i, \Gamma_i)\}_{i \in I}$ for some indexing set $I$. Let

$$B = \bigcup_{i \in I} B_i \quad \text{and} \quad \Gamma = \bigcup_{i \in I} \Gamma_i.$$

If $C, C' \in \Gamma$, $C \neq C'$, then there exists some indices $i, j$ such that $C \in \Gamma_i$ and $C' \in \Gamma_j$. Since $T$ is totally ordered, we have, say,

$$(B_i, \Gamma_i) \leqq (B_j, \Gamma_j).$$

Hence in fact, $C, C'$ are both elements of $\Gamma_j$, and hence $C, C'$ have an empty intersection. On the other hand, if $x \in B$, then $x \in B_i$ for some $i$, and hence there is some $C \in \Gamma_i$ such that $x \in C$. Hence $\Gamma$ is a disjoint covering of $B$. Since the

elements of each $\Gamma_i$ are denumerable subsets of $A$, it follows that $\Gamma$ is a disjoint covering of $B$ by denumerable sets, so $(B, \Gamma)$ is in $S$, and is obviously an upper bound for $T$. Therefore $S$ is inductively ordered.

Let $(M, \Delta)$ be a maximal element of $S$, by Zorn's lemma. Suppose that $M \neq A$. If the complement of $M$ in $A$ is infinite, then there exists a denumerable set $D$ contained in this complement. Then

$$(M \cup D, \Delta \cup \{D\})$$

is a bigger pair than $(M, \Delta)$, contradicting the maximality of $(M, \Delta)$. Hence the complement of $M$ in $A$ is a finite set $F$. Let $D_0$ be an element of $\Delta$. Let

$$D_1 = D_0 \cup F.$$

Then $D_1$ is denumerable. Let $\Delta_1$ be the set consisting of all elements of $\Delta$, except $D_0$, together with $D_1$. Then $\Delta_1$ is a disjoint covering of $A$ by denumerable sets, as was to be shown.

**Theorem 3.3.** *Let $A$ be an infinite set, and let $D$ be a denumerable set. Then*

$$\text{card}(A \times D) = \text{card}(A).$$

*Proof.* By the lemma, we can write

$$A = \bigcup_{i \in I} D_i$$

as a disjoint union of denumerable sets. Then

$$A \times D = \bigcup_{i \in I} (D_i \times D).$$

For each $i \in I$, there is a bijection of $D_i \times D$ on $D_i$ by Proposition 1.5. Since the sets $D_i \times D$ are disjoint, we get in this way a bijection of $A \times D$ on $A$, as desired.

**Corollary 3.4.** *If $F$ is a finite non-empty set, then*

$$\text{card}(A \times F) = \text{card}(A).$$

*Proof.* We have

$$\text{card}(A) \leqq \text{card}(A \times F) \leqq \text{card}(A \times D) = \text{card}(A).$$

We can then use Theorem 3.1 to get what we want.

**Corollary 3.5.** *Let $A$, $B$ be non-empty sets, $A$ infinite, and suppose*

$$\text{card}(B) \leqq \text{card}(A).$$

*Then*

$$\text{card}(A \cup B) = \text{card}(A).$$

*Proof.* We can write $A \cup B = A \cup C$ for some subset $C$ of $B$, such that $C$ and $A$ are disjoint. (We let $C$ be the set of all elements of $B$ which are not elements of $A$.) Then $\text{card}(C) \leqq \text{card}(A)$. We can then construct an injection of $A \cup C$ into the product

$$A \times \{1, 2\}$$

of $A$ with a set consisting of 2 elements. Namely, we have a bijection of $A$ with $A \times \{1\}$ in the obvious way, and also an injection of $C$ into $A \times \{2\}$. Thus

$$\text{card}(A \cup C) \leqq \text{card}(A \times \{1, 2\}).$$

We conclude the proof by Corollary 3.4 and Theorem 3.1.

**Theorem 3.6.** *Let $A$ be an infinite set. Then*

$$\text{card}(A \times A) = \text{card}(A).$$

*Proof.* Let $S$ be the set consisting of pairs $(B, f)$ where $B$ is an infinite subset of $A$, and $f$ is a bijection of $B$ onto $B \times B$. Then $S$ is not empty because if $D$ is a denumerable subset of $A$, we can always find a bijection of $D$ on $D \times D$. If $(B, f)$ and $(B', f')$ are in $S$, we define $(B, f) \leqq (B', f')$ to mean $B \subset B'$, and the restriction of $f'$ to $B$ is equal to $f$. Then $S$ is partially ordered, and we contend that $S$ is inductively ordered. Let $T$ be a non-empty totally ordered subset of $S$, and say $T$ consists of the pairs $(B_i, f_i)$ for $i$ in some indexing set $I$. Let

$$M = \bigcup_{i \in I} B_i.$$

We shall define a bijection $g : M \to M \times M$. If $x \in M$, then $x$ lies in some $B_i$. We define $g(x) = f_i(x)$. This value $f_i(x)$ is independent of the choice of $B_i$ in which $x$ lies. Indeed, if $x \in B_j$ for some $j \in I$, then say

$$(B_i, f_i) \leqq (B_j, f_j).$$

By assumption, $B_i \subset B_j$, and $f_j(x) = f_i(x)$, so $g$ is well defined. To show $g$ is surjective, let $x, y \in M$ and $(x, y) \in M \times M$. Then $x \in B_i$ for some $i \in I$ and $y \in B_j$ for some $j \in I$. Again since $T$ is totally ordered, say $(B_i, f_i) \leqq (B_j, f_j)$. Thus $B_i \subset B_j$, and $x, y \in B_j$. There exists an element $b \in B_j$ such that

$$f_j(b) = (x, y) \in B_j \times B_j.$$

By definition, $g(b) = (x, y)$, so $g$ is surjective. We leave the proof that $g$ is injective to the reader to conclude the proof that $g$ is a bijection. We then see

that $(M, g)$ is an upper bound for $T$ in $S$, and therefore that $S$ is inductively ordered.

Let $(M, g)$ be a maximal element of $S$, and let $C$ be the complement of $M$ in $A$. If $\text{card}(C) \leqq \text{card}(M)$, then

$$\text{card}(A) = \text{card}(M \cup C) = \text{card}(M)$$

by Corollary 3.5, and hence $\text{card}(M) = \text{card}(A)$. Since $\text{card}(M) = \text{card}(M \times M)$, we are done with the proof in this case. If

$$\text{card}(M) \leqq \text{card}(C),$$

then there exists a subset $M_1$ of $C$ having the same cardinality as $M$. We consider

$$\begin{aligned}(M \cup M_1) \times (M \cup M_1) \\ = (M \times M) \cup (M_1 \times M) \cup (M \times M_1) \cup (M_1 \times M_1).\end{aligned}$$

By the assumption on $M$ and Corollary 3.5, the last three sets in parentheses on the right of this equation have the same cardinality as $M$. Thus

$$(M \cup M_1) \times (M \cup M_1) = (M \times M) \cup M_2$$

where $M_2$ is disjoint from $M \times M$, and has the same cardinality as $M$. We now define a bijection

$$g_1 : M \cup M_1 \to (M \cup M_1) \times (M \cup M_1).$$

We let $g_1(x) = g(x)$ if $x \in M$, and we let $g_1$ on $M_1$ be any bijection of $M_1$ on $M_2$. In this way we have extended $g$ to $M \cup M_1$, and the pair $(M \cup M_1, g_1)$ is in $S$, contradicting the maximality of $(M, g)$. The case $\text{card}(M) \leqq \text{card}(C)$ therefore cannot occur, and our theorem is proved (using Exercise 14 below).

**Corollary 3.7.** *If $A$ is an infinite set, and $A^{(n)} = A \times \cdots \times A$ is the product taken $n$ times, then*

$$\text{card}(A^{(n)}) = \text{card}(A).$$

*Proof.* Induction.

**Corollary 3.8.** *If $A_1, \ldots, A_n$ are non-empty sets with $A_n$ infinite, and*

$$\text{card}(A_i) \leqq \text{card}(A_n)$$

*for $i = 1, \ldots, n$, then*

$$\text{card}(A_1 \times \cdots \times A_n) = \text{card}(A_n).$$

*Proof.* We have

$$\text{card}(A_n) \leqq \text{card}(A_1 \times \cdots \times A_n) \leqq \text{card}(A_n \times \cdots \times A_n)$$

and we use Corollary 3.7 and the Schroeder-Bernstein theorem to conclude the proof.

**Corollary 3.9.** *Let $A$ be an infinite set, and let $\Phi$ be the set of finite subsets of $A$. Then*

$$\text{card}(\Phi) = \text{card}(A).$$

*Proof.* Let $\Phi_n$ be the set of subsets of $A$ having exactly $n$ elements, for each integer $n = 1, 2, \ldots$. We first show that $\text{card}(\Phi_n) \leqq \text{card}(A)$. If $F$ is an element of $\Phi_n$, we order the elements of $F$ in any way, say

$$F = \{x_1, \ldots, x_n\}.$$

and we associate with $F$ the element $(x_1, \ldots, x_n) \in A^{(n)}$,

$$F \mapsto (x_1, \ldots, x_n).$$

If $G$ is another subset of $A$ having $n$ elements, say $G = \{y_1, \ldots, y_n\}$, and $G \neq F$, then

$$(x_1, \ldots, x_n) \neq (y_1, \ldots, y_n).$$

Hence our map

$$F \mapsto (x_1, \ldots, x_n)$$

of $\Phi_n$ into $A^{(n)}$ is injective. By Corollary 3.7, we conclude that

$$\text{card}(\Phi_n) \leqq \text{card}(A).$$

Now $\Phi$ is the disjoint union of the $\Phi_n$ for $n = 1, 2, \ldots$ and it is an exercise to show that $\text{card}(\Phi) \leqq \text{card}(A)$ (cf. Exercise 1). Since

$$\text{card}(A) \leqq \text{card}(\Phi),$$

because in particular, $\text{card}(\Phi_1) = \text{card}(A)$, we see that our corollary is proved.

In the next theorem, we shall see that given a set, there always exists another set whose cardinality is bigger.

**Theorem 3.10.** *Let $A$ be an infinite set, and $T$ the set consisting of two elements $\{0, 1\}$. Let $M$ be the set of all maps of $A$ into $T$. Then*

$$\text{card}(A) \leqq \text{card}(M) \quad \textit{and} \quad \text{card}(A) \neq \text{card}(M).$$

*Proof.* For each $x \in A$ we let

$$f_x : A \to \{0, 1\}$$

be the map such that $f_x(x) = 1$ and $f_x(y) = 0$ if $y \neq x$. Then $x \mapsto f_x$ is obviously an injection of $A$ into $M$, so that $\text{card}(A) \leqq \text{card}(M)$. Suppose that

$$\text{card}(A) = \text{card}(M).$$

Let

$$x \mapsto g_x$$

be a bijection between $A$ and $M$. We define a map $h : A \to \{0, 1\}$ by the rule

$$h(x) = 0 \quad \text{if} \quad g_x(x) = 1,$$

$$h(x) = 1 \quad \text{if} \quad g_x(x) = 0.$$

Then certainly $h \neq g_x$ for any $x$, and this contradicts the assumption that $x \mapsto g_x$ is a bijection, thereby proving Theorem 3.10.

**Corollary 3.11.** *Let $A$ be an infinite set, and let $S$ be the set of all subsets of $A$. Then* $\text{card}(A) \leqq \text{card}(S)$ *and* $\text{card}(A) \neq \text{card}(S)$.

*Proof.* We leave it as an exercise. [*Hint*: If $B$ is a non-empty subset of $A$, use the characteristic function $\varphi_B$ such that

$$\varphi_B(x) = 1 \quad \text{if} \quad x \in B,$$

$$\varphi_B(x) = 0 \quad \text{if} \quad x \notin B.$$

What can you say about the association $B \mapsto \varphi_B$?]

## §4. WELL-ORDERING

An ordered set $A$ is said to be **well-ordered** if it is totally ordered, and if every non-empty subset $B$ has a least element, that is, an element $a \in B$ such that $a \leqq x$ for all $x \in B$.

**Example 1.** The set of positive integers $\mathbf{Z}^+$ is well-ordered. Any finite set can be well-ordered, and a denumerable set $D$ can be well-ordered: Any bijection of $D$ with $\mathbf{Z}^+$ will give rise to a well-ordering of $D$.

**Example 2.** Let $S$ be a well-ordered set and let $b$ be an element of some set, $b \notin S$. Let $A = S \cup \{b\}$. We define $x \leqq b$ for all $x \in S$. Then $A$ is totally ordered, and is in fact well-ordered.

*Proof.* Let $B$ be a non-empty subset of $A$. If $B$ consists of $b$ alone, then $b$ is a least element of $B$. Otherwise, $B$ contains some element $a \in A$. Then $B \cap A$ is not empty, and hence has a least element, which is obviously also a least element for $B$.

**Theorem 4.1.** *Every non-empty set can be well-ordered.*

*Proof.* Let $A$ be a non-empty set. Let $S$ be the set of all pairs $(X, \omega)$, where $X$ is a subset of $A$ and $\omega$ is a well-ordering of $X$. Note that $S$ is not empty because any single element of $A$ gives rise to such a pair. If $(X, \omega)$ and $(X', \omega')$ are such pairs, we define $(X, \omega) \leqq (X', \omega')$ if $X \subset X'$, if the ordering induced on $X$ by $\omega'$ is equal to $\omega$, and if $X$ is an initial segment of $X'$. It is obvious that this defines an ordering on $S$, and we contend that $S$ is inductively ordered. Let $\{(X_i, \omega_i)\}$ be a totally ordered non-empty subset of $S$. Let $X = \bigcup X_i$. If $a, b \in X$, then $a, b$ lie in some $X_i$, and we define $a \leqq b$ in $X$ if $a \leqq b$ with respect to the ordering $\omega_i$. This is independent of the choice of $i$ (immediate from the assumption of total ordering). In fact, $X$ is well ordered, for if $Y$ is a non-empty subset of $X$, then there is some element $y \in Y$ which lies in some $X_j$. Let $c$ be a least element of $X_j \cap Y$. One verifies at once that $c$ is a least element of $Y$. We can therefore apply Zorn's lemma. Let $(X, \omega)$ be a maximal element in $S$. If $X \neq A$, then, using Example 2, we can define a well-ordering on a bigger subset than $X$, contradicting the maximality assumption. This proves Theorem 4.1.

**Note.** Theorem 4.1 is an immediate and straightforward consequence of Zorn's lemma. Usually in mathematics, Zorn's lemma is the most efficient tool when dealing with infinite processes.

## EXERCISES

1. Prove the statement made in the proof of Corollary 3.9.
2. If $A$ is an infinite set, and $\Phi_n$ is the set of subsets of $A$ having exactly $n$ elements, show that

$$\text{card}(A) \leqq \text{card}(\Phi_n)$$

for $n \geqq 1$.

3. Let $A_i$ be infinite sets for $i = 1, 2, \ldots$ and assume that

$$\text{card}(A_i) \leqq \text{card}(A)$$

for some set $A$, and all $i$. Show that

$$\text{card}\left(\bigcup_{i=1}^{\infty} A_i\right) \leqq \text{card}(A).$$

4. Let $K$ be a subfield of the complex numbers. Show that for each integer $n \geqq 1$, the cardinality of the set of extensions of $K$ of degree $n$ in $\mathbf{C}$ is $\leqq \text{card}(K)$.

5. Let $K$ be an infinite field, and $E$ an algebraic extension of $K$. Show that

$$\text{card}(E) = \text{card}(K).$$

6. Finish the proof of the Corollary 3.11.

7. If $A$, $B$ are sets, denote by $M(A, B)$ the set of all maps of $A$ into $B$. If $B$, $B'$ are sets with the same cardinality, show that $M(A, B)$ and $M(A, B')$ have the same cardinality. If $A$, $A'$ have the same cardinality, show that $M(A, B)$ and $M(A', B)$ have the same cardinality.

8. Let $A$ be an infinite set and abbreviate $\text{card}(A)$ by $\alpha$. If $B$ is an infinite set, abbreviate $\text{card}(B)$ by $\beta$. Define $\alpha\beta$ to be $\text{card}(A \times B)$. Let $B'$ be a set disjoint from $A$ such that $\text{card}(B) = \text{card}(B')$. Define $\alpha + \beta$ to be $\text{card}(A \cup B')$. Denote by $B^A$ the set of all maps of $A$ into $B$, and denote $\text{card}(B^A)$ by $\beta^\alpha$. Let $C$ be an infinite set and abbreviate $\text{card}(C)$ by $\gamma$. Prove the following statements:
   (a) $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$.
   (b) $\alpha\beta = \beta\alpha$.
   (c) $\alpha^{\beta+\gamma} = \alpha^\beta \alpha^\gamma$.

9. Let $K$ be an infinite field. Prove that there exists an algebraically closed field $K^a$ containing $K$ as a subfield, and algebraic over $K$. [*Hint*: Let $\Omega$ be a set of cardinality strictly greater than the cardinality of $K$, and containing $K$. Consider the set $S$ of all pairs $(E, \varphi)$ where $E$ is a subset of $\Omega$ such that $K \subset E$, and $\varphi$ denotes a law of addition and multiplication on $E$ which makes $E$ into a field such that $K$ is a subfield, and $E$ is algebraic over $K$. Define a partial ordering on $S$ in an obvious way; show that $S$ is inductively ordered, and that a maximal element is algebraic over $K$ and algebraically closed. You will need Exercise 5 in the last step.]

10. Let $K$ be an infinite field. Show that the field of rational functions $K(t)$ has the same cardinality as $K$.

11. Let $J_n$ be the set of integers $\{1, \ldots, n\}$. Let $\mathbf{Z}^+$ be the set of positive integers. Show that the following sets have the same cardinality:
   (a) The set of all maps $M(\mathbf{Z}^+, J_n)$.
   (b) The set of all maps $M(\mathbf{Z}^+, J_2)$.
   (c) The set of all real numbers $x$ such that $0 \leqq x < 1$.
   (d) The set of all real numbers.

12. Show that $M(\mathbf{Z}^+, \mathbf{Z}^+)$ has the same cardinality as the real numbers.

13. Let $S$ be a non-empty set. Let $S'$ denote the product $S$ with itself taken denumerably many times. Prove that $(S')'$ has the same cardinality as $S'$. [Given a set $S$ whose cardinality is strictly greater than the cardinality of $\mathbf{R}$, I do not know whether it is always true that $\text{card } S = \text{card } S'$.] Added 1994: The grapevine communicates to me that according to Solovay, the answer is "no."

14. Let $A$, $B$ be non–empty sets. Prove that

$$\text{card}(A) \leqq \text{card}(B) \quad \text{or} \quad \text{card}(B) \leqq \text{card}(A).$$

[Hint: consider the family of pairs $(C, f)$ where $C$ is a subset of $A$ and $f: C \to B$ is an injective map. By Zorn's lemma there is a maximal element. Now finish the proof].

## Bibliography


[Ad 62] F. ADAMS, Vector Fields on Spheres, *Ann. Math.* **75** (1962) pp. 603–632

[Ara 31] H. ARAMATA, Über die Teilbarkeit der Dedekindschen Zetafunktionen, *Proc. Imp. Acad. Tokyo* **7** (1931) pp. 334–336

[Ara 33] H. ARAMATA, Über die Teilbarkeit der Dedekindschen Zetafunktionen, *Proc. Imp. Acad. Tokyo* **9** (1933) pp. 31–34

[Art 24] E. ARTIN, Kennzeichnumg des Körpers der reellen algebraischen Zahlen, *Abh. Math. Sem. Hansischen Univ.* **3** (1924) pp. 319–323

[Art 27] E. ARTIN, Über die Zerlegung definiter Funktionen in Quadrate, *Abh. Math. Sem. Hansischen Univ.* **5** (1927) pp. 100–115

[Art 44] E. ARTIN, *Galois Theory*, University of Notre Dame, 1944

[ArS 27] E. ARTIN and E. SCHREIER, Algebraische Konstruktion reeller Körper, *Abh. Math. Sem. Hansischen Univ.* **5** (1927) pp. 85–99

[ArT 68] E. ARTIN and J. TATE, *Class Field Theory*, Benjamin-Addison Wesley, 1968 (reprinted by Addison-Wesley, 1991)

[Art 68] M. ARTIN, On the solutions of analytic equations, *Invent. Math.* **5** (1968) pp. 277–291

[ArM 65] M. ARTIN and B. MAZUR, On periodic points, *Ann. Math. (2)* **81** (1965) pp. 89–99

[At 61] M. ATIYAH, Characters and cohomology of finite groups, *Pub. IHES* **9** (1961) pp. 5–26

[At 67] M. ATIYAH, *K-Theory*, Addison-Wesley, (reprinted from the Benjamin Lecture Notes, 1967)

[ABP 73] M. ATIYAH, R. BOTT, V. PATODI, On the heat equation and the index theorem, *Invent. Math.* **19** (1973) pp. 270–330

[ABS 64] M. ATIYAH, R. BOTT, A. SHAPIRO, Clifford Modules, *Topology* **Vol. 3 Supp. 1** (1964) pp. 3–38

[AtM 69] M. ATIYAH and I. MCDONALD, *Introduction to commutative algebra*, Addison-Wesley, 1969

[Ba 68] H. BASS, *Algebraic K-theory*, Benjamin, 1968

[BaH 62] P. T. BATEMAN and R. HORN, A heuristic asymptotic formula concerning the distribution of prime numbers, *Math. Comp.* **16** (1962) pp. 363–367

[Be 80] G. BELYI, Galois extensions of the maximal cyclotomic field, *Izv. Akad. Nauk SSSR* **43** (1979) pp. 267–276 (= *Math. USSR Izv.* **14** (1980), pp. 247–256

[Be 83] G. BELYI, On extensions of the maximal cyclotomic field having a given classical Galois group, *J. reine angew. Math.* **341** (1983) pp. 147–156

[BeY 91] C. BERENSTEIN and A. YGER, Effective Bezout identities in $\mathbb{Q}[z_1, \ldots z_n]$, *Acta Math.* **166** (1991) pp. 69–120

[BGV 92] N. BERLINE, E. GETZLER, M. VERGNE, *Heat kernels and Dirac operators*, Springer-Verlag, 1992

[BCHS 65] B. BIRCH, S. CHOWLA, M. HALL, and A. SCHINZEL, On the difference $x^3 - y^2$, *Norske Vid. Selsk. Forrh.* **38** (1965) pp. 65–69

[Bott 69] R. BOTT, *Lectures on K(X)*, Benjamin 1969

[Boun 1854] V. BOUNIAKOWSKY, Sur les diviseurs numériques invariables des fonctions

rationnelles entières, *Mémoires sc. math. et phys.* **T. VI** (1854–1855) pp. 307–329

[Bour 82] N. BOURBAKI, *Lie algebras and Lie groups*, Masson, 1982

[Bra 47a] R. BRAUER, On the zeta functions of algebraic number fields, *Amer. J. Math.* **69** (1947) pp. 243–250

[Bra 47b] R. BRAUER, On Artin's L-series with general group characters, *Ann. Math.* **48** (1947) pp. 502–514

[BLSTW 83] J. BRILLHART, D. H. LEHMER, J. L. SELFRIDGE, B. TUCKERMAN, and S. WAGSTAFF, Factorization of $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11$ up to high powers, *Contemporary Mathematics* **Vol. 22**, AMS, Providence, RI, 1983

[BtD 85] T. BRÖCKER and T. TOM DIECK, *Representations of Compact Lie Groups*, Springer-Verlag, 1985

[Br 87] D. BROWNAWELL, Bounds for the degree in Nullstellensatz, *Ann. of Math.* **126** (1987) pp. 577–592

[Br 88] D. BROWNAWELL, Local diophantine nullstellen inequalities, *J. Amer. Math. Soc.* **1** (1988) pp. 311–322

[Br 89] D. BROWNAWELL, Applications of Cayley-Chow forms, *Springer Lecture Notes* **1380**: *Number Theory, Ulm*, 1987, H. P. Schlickewei and E. Wirsing (eds.) pp. 1–18

[BrCDT 01] C. BREUIL, B. CONRAD, F. DIAMOND, R. TAYLOR, On the modularity of elliptic curves over **Q**: Wild 3-adic exercises, *J. Amer. Math. Soc.* **14** (2001) pp. 843–939

[CaE 57] E. CARTAN and S. EILENBERG, Homological Algebra, Princeton University Press, 1957

[CCFT 91] P. CASSOU-NOGUES, T. CHINBURG, A. FROLICH, M. J. TAYLOR, L-functions and Galois modules, in *L-functions and Arithmetic*, J. Coates and M. J. Taylor (eds.), Proceedings of the Durham symposium July 1989, *London Math. Soc. Lecture Notes Series* **153**, Cambridge University Press (1991) pp. 75–139

[CuR 81] C. W. CURTIS and I. REINER, *Methods of Representation Theory*, John Wiley and Sons, 1981

[Da 65] H. DAVENPORT, On $f^3(t) - g^2(t)$, *Norske Vid. Selsk. Forrh.* **38** (1965) pp. 86–87

[De 68] P. DELIGNE, Formes modulaires et représentations $l$-adiques, *Séminaire Bourbaki* 1968–1969, pp. 55–105

[De 73] P. DELIGNE, Formes modulaires et représentations de GL(2), *Springer Lecture Notes* **349** (1973) pp. 507–530

[DeS 74] P. DELIGNE and J.-P. SERRE, Formes modulaires de poids 1, *Ann. Sci. ENS* **7** (1974) pp. 507–530

[Dou 64] A. DOUADY, Determination d'un groupe de Galois, *C.R. Acad. Sci.* **258** (1964), pp. 5305–5308

[ES 52] S. EILENBERG and N. STEENROD, *Foundations of Algebraic Topology*, Princeton University Press, 1952

[Fa 91] G. FALTINGS, *Lectures on the arithmetic Riemann-Roch theorem*, Ann. Math. Studies **127**, 1991

[Fr 87] G. FREY, Links between stable elliptic curves and certain diophantine equations, *Number Theory, Lecture Notes* **1380**, Springer-Verlag 1987 pp. 31–62

[Fro 83] A. FRÖLICH, *Galois Module Stuctures of Algebraic Integers*, Ergebnisse der Math. 3 Folge Vol. 1, Springer-Verlag (1983)

[FuL 85] W. FULTON and S. LANG, Riemann-Roch Algebra, Springer-Verlag, 1985

[God 58] R. GODEMENT, *Théorie des faisceaux*, Hermann Paris, 1958

[Gor 68] D. GORENSTEIN, *Finite groups*, Harper and Row, 1968

[Gor 82] D. GORENSTEIN, *Finite simple groups*, Plenum Press, 1982

[Gor 83] D. GORENSTEIN, The classification of finite simple groups, Plenum Press, 1983

[Gor 86] D. GORENSTEIN, Classifying the finite simple groups, *Bull. AMS* **14** No. 1 (1986) pp. 1–98

[GreH 81] M. GREENBERG and J. HARPER, *Algebraic Topology: A First Course*, Benjamin-Addison Wesley, 1981

[GriH 78] P. GRIFFITHS and J. HARRIS, *Principles of Algebraic Geometry*, Wiley Interscience, New York, 1978

[Gro 57] A. GROTHENDIECK, Sur quelques points d'algèbre homologique, *Tohoku Math. J.* **9** (1957) pp. 119–221

[Gro 68] A. GROTHENDIECK, Classes de Chern et représentations linéaires des groupes discrets, *Dix exposés sur la cohomologie étale des schémas*, North-Holland, Amsterdam, 1968

[Gu 90] R. GUNNING, *Introduction to Holomorphic Functions of Several Variables*, Vol. II: Local Theory; Vol. III, Wadsworth and Brooks/Cole, 1990

[HalR 74] H. HALBERSTAM and H.-E. RICHERT, Sieve methods, Academic Press, 1974

[Hal 71] M. HALL, The diophantine equation $x^3 - y^2 = k$, *Computers and Number Theory*, ed. by A. O. L. Atkin and B. Birch, Academic Press, London 1971 pp. 173–198

[HardW 71] G. H. HARDY and E. M. WRIGHT, *An Introduction to the Theory of Numbers*, Oxford University Press, Oxford, UK, 1938–01971 (several editions)

[Hart 77] R. HARTSHORNE, *Algebraic Geometry*, Springer-Verlag, New York, 1977

[Has 34] H. HASSE, Abstrakte Begrundung der komplexen Multiplikation und Riemannsche Vermutung in Funktionenkörpern, *Abh. Math. Sem. Univ. Hamburg* **10** (1934) pp. 325–348

[HilS 70] P. J. HILTON and U. STAMMBACH, *A course in homological algebra*, Graduate Texts in Mathematics, Springer-Verlag 1970

[Hir 66] F. HIRZEBRUCH, *Topological methods in algebraic geometry*, Springer-Verlag, New York, 1966 (Translated and expanded from the original German, 1956)

[Hu 75] D. HUSEMOLLER, *Fibre Bundles*, Springer-Verlag, second edition, 1975

[Ih 66] Y. IHARA, On discrete subgroups of the two by two projective linear group over $p$-adic fields, *J. Math Soc. Japan* **18** (1966) pp. 219–235

[Ik 77] M. IKEDA, Completeness of the absolute Galois group of the rational number field, *J. reine angew. Math.* **291** (1977) pp. 1–22

[Iw 53] K. IWASAWA, On solvable extensions of algebraic number fields, *Ann. Math.* **548** (1953) pp. 548–572

[Ja 79] N. JACOBSON, *Lie algebras*, Dover, 1979 (reprinted from Interscience, 1962)

[Ja 85] N. JACOBSON, *Basic Algebra* I and II, second edition, Freeman, 1985

[JoL 01] J. JORGENSON and S. LANG, *Spherical Inversion on $SL_n(\mathbf{R})$*, Springer Verlag 2001

[Jou 80] J.-P. JOUANOLOU, Idéaux résultants, *Advances in Mathematics* **37 No. 3** (1980) pp. 212–238

[Jou 90] J.-P. JOUANOLOU, Le formalisme du résultant, *Advances in Mathematics* **90 No. 2** (1991) pp. 117–263

[Jou 91] J.-P. JOUANOLOU, *Aspects invariants de l'élimination*, Département de Mathématiques, Université Louis Pasteur, Strasbourg, France (1991)

[Ko 88] J. KOLLAR, Sharp effective nullstellensatz, *J. Amer. Math. Soc.* **1 No. 4** (1988) pp. 963–975

[Kr 32] W. KRULL, Allgemeine Bewertungstheorie, *J. reine angew. Math.* (1932) pp. 169–196

[La 52] S. LANG, On quasi algebraic closure, *Ann. Math.* **55** (1952) pp. 373–390

[La 53] S. LANG, The theory of real places, *Ann. Math.* **57** No. 2 (1953) pp. 378–391

[La 58] S. LANG, *Introduction to Algebraic Geometry*, Interscience, 1958

[La 70] S. LANG, *Algebraic Number Theory*, Addison-Wesley, 1970; reprinted by Springer-Verlag; second edition 1994

[La 72] S. LANG, *Differential Manifolds*, Addison-Wesley, 1972; reprinted by Springer-Verlag, 1985; superceded by [La 99a]

[La 73] S. LANG, *Elliptic Functions*, Springer-Verlag, 1973; second edition 1987

[La 76] S. LANG, *Introduction to Modular Forms*, Springer-Verlag 1976

[La 78] S. LANG, Elliptic Curves: Diophantine Analysis, Springer 1978

[La 82] S. LANG, Units and class groups in number theory and algebraic geometry, *Bull. AMS* **Vol. 6 No. 3** (1982) pp. 253–316

[La 83] S. LANG, *Fundamentals of Diophantine Geometry*, Springer-Verlag 1983

[La 85] S. LANG, *Real Analysis*, Second edition, Addison-Wesley, 1985; third edition *Real and Functional Analysis*, Springer-Verlag, 1993

[La 90a] S. LANG, *Undergraduate Algebra*, second edition, Springer-Verlag, 1990

[La 90b] S. LANG, *Cyclotomic fields, I and II*, Springer-Verlag, New York, 1990, combined edition of the original editions, 1978, 1980

[La 90c] S. LANG, Old and new conjectured diophantine inequalities, *Bull. AMS* **Vol. 23 No. 1** (1990) pp. 37–75

[La 96] S. LANG, *Topics in Cohomology of Groups*, Springer Lecture Notes 1996, reproduced in Lang's *Collected Papers*, Vol. IV, Springer 2000

[La 99a] S. LANG, *Fundamentals of Differential Geometry*, Springer Verlag, 1999

[La 99b] S. LANG, *Math Talks for Undergraduates*, Springer Verlag, 1999

[LaT 75] S. LANG and H. TROTTER, *Distribution of Frobenius Elements in $GL_2$-Extensions of the Rational Numbers*, Springer Lecture Notes **504**

[Ma 16] F. MACAULAY, *The algebraic theory of modular systems*, Cambridge University Press, Cambridge UK, 1916

[Mack 51] G. MACKEY, On induced representations of groups, *Amer. J. Math.* **73** (1951) pp. 576–592

[Mack 53] G. MACKEY, Symmetric and anti-symmetric Kronecker squares of induced representations of finite groups, *Amer. J. Math.* **75** (1973) pp. 387–405

[Man 69] J. MANIN, *Lectures on the K-functor in algebraic geometry*, Russian Math. Surveys 24(5) (1969) pp. 1–89

[Man 71] A. MANNING, Axiom A diffeomorphisms have rational zeta functions, *Bull. Lond. Math. Soc.* **3** (1971) pp. 215–220

[Mas 84a] R. C. MASON, Equations over function fields, Springer Lecture Notes **1068** (1984) pp. 149–157; in *Number Theory, Proceedings of the Noordwijkerhout*, 1983

[Mas 84b] R. C. MASON, Diophantine equations over function fields, *London Math. Soc. Lecture Note Series* **Vol. 96**, Cambridge University Press, 1984

[Mas 84c] R. C. MASON, The hyperelliptic equation over function fields, *Math. Proc. Cambridge Philos. Soc.* **93** (1983) pp. 219–230

[MaW 85] D. MASSER and G. WÜSTHOLZ, Zero estimates on group varieties II, *Invent. Math.* **80** (1985) pp. 233–267

[Mat 80] H. MATSUMURA, *Commutative algebra*, second edition, Benjamin-Cummings, New York 1980

[Mat 86] H. MATSUMURA, *Commutative rings*, Cambridge University Press, 1986

[Matz 87] B. MATZAT, Konstruktive Galoistheorie, Springer Lecture Notes **1284**, 1987

[Matz 88] B. MATZAT, Über das Umkehrproblem der Galoischen Theorie, *Jahrsbericht Deutsch. Mat.-Verein.* **90** (1988) pp. 155–183

[Neu 69a] J. NEUKIRCH, Über eine algebraische Kennzeichnung der Henselkörper, *J. reine angew. Math.* **231** (1968) pp. 75–81

[Neu 69b] J. NEUKIRCH, Kennzeichnung der $p$-adischen und endlichen algebraischen Zahlkörper, *Invent. Math.* **6** (1969) pp. 269–314

[Neu 69c] J. NEUKIRCH, Kennzeichnung der endlich-algebraischen Zahlkörper durch die Galoisgruppe der maximal auflösbaren Erweiterungen, *J. fur Math.* **238** (1969) pp. 135–147

[No 76] D. NORTHCOTT, *Finite Free Resolutions*, Cambridge University Press, 1976

[Ph 86] P. PHILIPPON, Lemmes de zéros dans les groupes algébriques commutatifs, *Bull. Soc. Math. France* **114** (1986) pp. 355–383

[Ph 91–95] P. PHILIPPON, Sur des hauteurs alternatives I, *Math. Ann.* **289** (1991) pp. 255–283; II Ann. Inst. Fourier 44 (1994) pp. 1043–1065; III J. Math. Pures Appl. 74 (1995) pp. 345–365

[Pop 94] F. POP, On Grothendieck's conjecture of birational anabelian geometry, *Annals of Math.* (2) **139** (1994) pp. 145–182

[Pop 95] F. POP, Etale Galois covers of affine smooth curves, *Invent. Math.* **120** (1995), pp. 555–578

[Ri 90a] K. RIBET, On modular representations of $\mathrm{Gal}(\mathbf{Q}^a/\mathbf{Q})$ arising from modular forms, *Invent. Math.* **100** (1990) pp. 431–476

[Rib 90b] K. RIBET, From the Taniyama-Shimura conjecture to Fermat's last theorem, *Annales de la Fac. des Sci. Toulouse* (1990) pp. 116–170

[Ric 60] C. RICKART, *Banach Algebras*, Van Nostrand (1960), Theorems 1.7.1 and 4.2.2

[Ro 79] J. ROTMAN, *Introduction to Homological Algebra*, Academic Press, 1979

[Ru 73] W. RUDIN, *Functional Analysis*, McGraw Hill (1973) Theorems 10.14, and 11.18

[Schi 58] A. SCHINZEL and W. SIERPINSKI, Sur certaines hypothèses concernant les nombres premiers, *Acta Arith.* **4** (1948) pp. 185–208

[Schulz 37] W. SCHULZ, Über die Galoissche Gruppe der Hermitschen Polynome, *J. reine angew. math.* **177** (1937) pp. 248–252

[Schur 31] J. SCHUR, Affektlose Gleichungen in der Theorie der Laguereschen und Hermiteschen Polynome, *J. reine angew. math.* **165** (1931) pp. 52–58

[Se 62] J.-P. SERRE, Endomorphismes complètements continus des espaces de Banach p-adiques, *Pub. Math. IHES* **12** (1962) pp. 69–85

[Se 64] J.-P. SERRE, *Cohomologie Galoisienne*, Springer Lecture Notes **5**, 1964

[Se 65a] J.-P. SERRE, *Algèbre locale, multiplicités*, Springer Lecture Notes **11** (1965) Third Edition 1975

[Se 65b] J.-P. SERRE, *Lie algebras and Lie groups*, Benjamin, 1965; reprinted *Springer Lecture Notes* **1500**, Springer-Verlag 1992

[Se 68a] J.-P. SERRE, *Abelian l-adic representations and Elliptic Curves*, Benjamin, 1968

[Se 68b] J.-P. SERRE, Une interprétation des congruences relatives à la fonction de Ramanujan, *Séminaire Delange-Poitou-Pisot*, 1971–1972

[Se 72a] J.-P. SERRE, Propriétés Galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972) pp. 259–331

[Se 72b] J.-P. SERRE, Congruences et formes modulaires (d'après Swinnerton-Dyer), *Séminaire Bourbaki*, 1971–1972

[Se 73] J.-P. SERRE, *A Course in Arithmetic*, Springer-Verlag, New York, 1973

[Se 80] J.-P. SERRE, *Trees*, Springer-Verlag, 1980

[Se 87] J.-P. SERRE, Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\mathbf{Q}^a/\mathbf{Q})$, *Duke Math. J.* **54** (1987), pp. 179–230

[Se 88] J.-P. SERRE, Groupes de Galois sur **Q**, *Séminaire Bourbaki*, 1987–1988, *Astérisque* **161–162**, pp. 73–85

[Se 92] J.-P. SERRE, *Topics in Galois theory*, course at Harvard, 1989, Jones and Bartlett, Boston 1992

[SGA 6] P. BERTHELOT, A. GROTHENDIECK, L. ILLUSIE et al., *Théorie des intersections et théorème de Riemann-Roch*, Springer Lecture Notes **146** (1967)

[Shaf 54] I. SHAFAREVICH, Construction of fields of algebraic number with given solvable Galois group, *Izv. Akad. Nauk SSSR* **18** (1954) pp. 525–578 (*Amer. math. Soc. Transl.* **4** (1956)) pp. 185–237

[Shat 72] S. SHATZ, *Profinite groups, arithmetic and geometry*, Ann. of Math. Studies, Princeton University Press 1972

[Shih 74] R.-Y. SHIH, On the construction of Galois extensions of function fields and number fields, *Math. Ann.* **207** (1974), pp. 99–120

[Shim 66] G. SHIMURA, A Reciprocity law in non-solvable extensions, *J. reine angew. Math.* **224** (1966) pp. 209–220

[Shim 71] G. SHIMURA, *Introduction to the arithmetic theory of Automorphic Functions*, Iwanami Shoten and Princeton University Press, 1971

[Shu 87] M. SHUB, *Global Stability of Dynamical Systems*, Springer-Verlag, New York 1987

[Sil 88] J. SILVERMAN, Wieferich's criterion and the *abc* conjecture, *J. Number Theory* **30** (1988) pp. 226–237

[Sn 00] N. SNYDER, An alternate proof of Mason's theorem, *Elemente der Math.* **55** (2000) pp. 93–94

[Sol 01] R. SOLOMON, A brief history of the classification of the finite simple groups, *Bull. AMS* Vol. **38** No. 3 (2001) pp. 315–322

[Sou 90] C. SOULÉ, Géometrie d'Arakelov et théorie des nombres transcendants, Preprint, 1990

[SteT 86] C.L. STEWART and R. TIJDEMAN, On the Oesterle–Masser Conjecture, *Mon. Math.* **102** (1986) pp. 251–257

[Sto 81] W. STOTHERS, Polynomial identites and hauptmoduln, *Quart. J. Math. Oxford* (2) **32** (1981) pp. 349–370

[Sw 69] R. SWAN, Invariant rational functions and a problem of Steenrod, *Invent. Math.* **7** (1969) pp. 148–158

[Sw 83] R. SWAN, Noether's problem in Galois theory, *Emmy Noether in Bryn Mawr*, J. D. Sally and B. Srinivasan, eds., Springer-Verlag, 1983, p. 40

[SwD 73] H. P. SWINNERTON-DYER, On $l$-adic representations and congruences for coefficients of modular forms, Antwerp conference, *Springer Lecture Notes* **350** (1973)

[TaW 95] R. TAYLOR and A. WILES, Ring-theoretic properties of certain Hecke algebras, *Annals of Math.* **141** (1995) pp. 553–572

[Uch 77] K. UCHIDA, Isomorphisms of Galois groups of algebraic function fields, *Ann. of Math.* **106** (1977) pp. 589–598

[Uch 79] K. UCHIDA, Isomorphisms of Galois groups of solvable closed Galois extensions, *Tohoku Math. J.* **31** (1979) pp. 359–362

[Uch 81] K. UCHIDA, Homomorphisms of Galois groups of solvably closed Galois extensions, *J. Math. Soc. Japan* **33** (1981) pp. 595–604

[vdW 29] B. L. VAN DER WAERDEN, On Hilbert's function, series of composition of ideals and a generalization of the theorem of Bezout, *Proc. R. Soc. Amsterdam* **31** (1929) pp. 749–770

[vdW 30] B. L. VAN DER WAERDEN, *Modern Algebra*, Springer-Verlag, 1930

[Wil 95] A. WILES, Modular elliptic curves and Fermat's last theorem, *Annals of Math.* **141** (1995) pp. 443–551

[Win 91] K. WINBERG, On Galois groups of $p$-closed algebraic number fields with restricted ramification, I, *J. reine angew. Math.* **400** (1989) pp. 185–202 and II, *ibid.* **416** (1991) pp. 187–194

[Wit 35] E. WITT, Der Existenzsatz für abelsche Funktionenkörper, *J. reine angew. Math.* **173** (1936) pp. 43–51

[Wit 36] E. WITT, Konstruktion von galoisschen Körpern der Charakteristik $p$ mit vorgegebener Gruppe der Ordnung $p^f$, *J. reine angew. Math.* **174** (1936) pp. 237–245

[Wit 37] E. WITT, Zyklische Körper und Algebren der Charakteristik $p$ vom Grad $p^n$. Struktur diskret bewerteter perfekter Körper mit vollkommenem Restklassenkörper der Charakteristik $p$, *J. reine angew. Math.* **176** (1937) pp. 126–140

[Za 95] U. ZANNIER, On Davenport's bound for the degree of $f^3 - g^2$ and Riemann's existence theorem, *Acta Arithm.* **LXXI.2** (1995) pp. 107–137

# INDEX


*abc* conjecture, 195
abelian, 4
  category, 133
  extension, 266, 278
  group, 4, 42, 79
  Kummer theory, 293
  tower, 18
absolute value, 465
absolutely semisimple, 659
abstract nonsense, 759
abut, 815
action of a group, 25
acyclic, 795
Adams operations, 726, 782
additive category, 133
additive functor, 625, 790
additive polynomial, 308
adic
  completion, 163, 206
  expansion, 190
  topology, 162, 206
adjoint, 533, 581
affine space, 383
algebra, 121, 629, 749
algebraic
  closure, 178, 231, 272
  element, 223
  extension, 224
  group, 549
  integer, 371
  set, 379
  space, 383, 386
algebraically
  closed, 272
  independent, 102, 308, 356
almost all, 5
alternating
  algebra, 733
  form, 511, 526, 530, 571, 598
  group, 31, 32, 722
  matrix, 530, 587
  multilinear map, 511, 731
  product, 733, 780
annihilator, 417
anti-dual, 532
anti-linear, 562
anti-module, 532
approximation theorem, 467
Aramata's theorem, 701
archimedean ordering, 450
Artin
  conjectures, 256, 301
  theorems, 264, 283, 290, 429
artinian, 439, 443, 661
Artin-Rees theorem, 429
Artin-Schreier theorem, 290
associated
  graded ring, 428, 430
  group and field, 301
  ideal of algebraic set, 381
  linear map, 507
  matrix of bilinear map, 528
  object, 814
  prime, 418
associative, 3
asymptotic Fermat, 196
automorphism, 10, 54
  inner, 26
  of a form, 525, 533

Banach space, 475
balanced, 660
base change, 625
basis, 135, 140
Bateman-Horn conjecture, 323
belong
  group and field, 263
  ideal and algebraic set, 381
  prime and primary ideal, 421
Bernoulli
  numbers, 218
  polynomials, 219
bifunctor, 806
bijective, ix
bilinear form, 146, 522

bilinear map, 48, 121, 144
binomial polynomial, 434
Blichfeldt theorem, 702
blocks, 555
Borel subgroup, 537
boundaries, 767
bounded complex, 762
Bourbaki theorems
  on sets, 881
  on traces and semisimplicity, 650
bracket product, 121
Brauer's theorems, 701, 709
Bruhat decomposition, 539
Burnside theorems
  on simple modules, 648
  on tensor representations, 726
butterfly lemma, 20

$\mathfrak{C}$-dimension, 772
cancellation law, 40
canonical map, 14, 16
cardinal number, 885
Cartan subgroup, 712
Casimir, 628, 639
category, 53
Cauchy
  family, 52
  sequence, 51, 162, 206, 469
Cayley-Hamilton theorem, 561
center
  of a group, 26, 29
  of a ring, 84
central element, 714
centralizer, 14
chain condition, 407
character, 282, 327, 667, 668
  independence, 283, 676
characteristic, 90
characteristic polynomial, 256, 434, 561
  of tensor product, 569
Chevalley's theorem, 214
Chinese remainder theorem, 94
class formula, 29
class function, 673
class number, 674
Clifford algebra, 749, 757
closed
  complex, 765
  subgroup, 329
  under law of composition, 6
coboundary, 302
cocycle
  $GL_n$, 549
  Hilbert's theorem, 90, 288
  Sah's theorem, 303
coefficient function, 681
coefficients
  of linear combination, 129
  of matrix, 503
  of polynomial, 98, 101
coerasable, 805
cofinal, 52
cohomology, 288, 302, 303, 549, 764
  of groups, 826
cokernel, 119, 133
column
  operation, 154
  rank, 506
  vector, 503
commutative, 4
  diagram, ix
  group, 4
  ring, 83, 84, 86
commutator, 20, 69, 75
commutator subgroup, 20, 75
  of $SL_n$, 539, 541
commute, 29
compact
  Krull topology, 329
  spec of a ring, 411
complete
  family, 837
  field, 469
  ring and local ring, 206
completely reducible, 554
completion, 52, 469, 486
complex, 445, 761, 765
complex numbers, 272
component, 503, 507
  of a matrix, 503
composition of mappings, 85
compositum of fields, 226
conjugacy class, 673
conjugate elements
  of a group, 26
  of a field, 243
conjugate
  embeddings, 243, 476
  fields, 243, 477
  subgroups, 26, 28, 35
conjugation, 26, 552, 570, 662
connected, 411
connected sum, 6
connection, 755

constant polynomial, 175
constant term, 100
content, 181
contragredient, 665
contravariant functor, 62
convergence, 206
convolution, 85, 116
coordinates, 408
coproduct, 59, 80
  of commutative rings, 630
  of groups, 70, 72
  of modules, 128
correspondence, 76
coset, 12
  representative, 12
countable, 878
covariant functor, 62
Cramer's rule, 513
cubic extension, 270
cuspidal, 318
cycle
  in homology, 767
  in permutations, 30
cyclic
  endomorphism, 96
  extension, 266, 288
  group, 8, 23, 96, 830
  module, 147, 149
  tower, 18
cyclotomic
  field, 277–282, 314, 323
  polynomials, 279

Davenport theorem, 195
decomposable, 439
decomposition
  field, 341
  group, 341
Dedekind
  determinant, 548
  ring, 88, 116, 168, 353
defined, 710, 769
definite form, 593
degree
  of extension, 224
  of morphism, 765
  of polynomial, 100, 190
  of variety, 438
  Weierstrass, 208
Deligne-Serre theorem, 319
density theorem, 647
denumerable set, 875
dependent absolute values, 465
de Rham complex, 748
derivation, 214, 368, 746, 754
  over a subfield, 369
  universal, 746
derivative, 178
derived functor, 791
descending chain condition, 408, 439, 443, 661
determinant, 513
  ideal, 738, 739
  of cohomology, 738
  of linear map, 513, 520
  of module, 735
  of Witt group, 595
diagonal element, 504
diagonalizable, 568
diagonalized form, 576
difference equations, 256
differential, 747, 762, 814
dihedral group, 78, 723
dimension
  of character, 670
  of module, 146, 507
  of transcendental extension, 355
  of vector space, 141
dimension in homology, 806, 811, 823
  shifting, 805
direct
  limit, 160, 170, 639
  product, 9, 127
  sum, 36, 130, 165
directed family, 51, 160
discrete valuation ring, 487
discriminant, 193, 204, 270, 325
distinguished extensions
  of fields, 227, 242
  of rings, 335, 291
distinguished polynomials, 209
distributivity, 83
divide, 111, 116
divisible, 50
division ring, 84, 642
Dolbeault complex, 764
dominate (polynomials), 870
double coset, 75, 693
doubly transitive, 80
dual
  basis, 142, 287
  group, 46, 145
  module, 142, 145, 523, 737
  representation, 665

effective character, 668, 685
eigenvalue, 562
eigenvector, 562, 582–585
Eisenstein criterion, 183
elementary
  divisors, 153, 168, 521, 547
  group, 705
  matrix, 540
  symmetric polynomials, 190, 217
elimination, 391
  ideal, 392
embedding, 11, 120
  of fields, 229
  of rings, 91
endomorphism, 10, 24, 54
  of cyclic groups, 96
enough
  injectives, 787
  T-exacts, 810
entire, 91
  functions, 87
epimorphism, 120
equivalent
  norms, 470
  places, 349
  valuations, 480
erasable, 800
euclidean algorithm, 173, 207
Euler characteristic, 769
Euler-Grothendieck group, 771
Euler phi function, 94
Euler-Poincaré
  characteristic, 769, 824
  map, 156, 433, 435, 770
evaluation, 98, 101
even permutation, 31
exact, 15, 120
  for a functor, 619
  sequence of complexes, 767
expansion of determinant, 515
exponent
  of an element, 23, 149
  of a field extension, 293
  of a group, 23
  of a module, 149
exponential, 497
Ext, 791, 808, 810, 831, 857
extension
  of base, 623
  of derivations, 375
  of fields, 223
  of homomorphisms, 347, 378
  of modules, 831
exterior
  algebra, 733
  product, 733
extreme point, 883

factor
  group, 14
  module, 119, 141
  ring, 89
factorial, 111, 115, 175, 209
faithful, 28, 334, 649, 664
faithfully flat, 638
Fermat theorem, 195, 319
fiber product, 61, 81
field, 93
  of definition of a representation, 710
filtered complex, 817
filtration, 156, 172, 426, 814, 817
finite
  complex, 762
  dimension, 141, 772, 823
  extension, 223
  field, 244
  free resolution, 840
  homological dimension, 772, 823
  module, 129
  resolution, 763
  sequence, 877
  set, 877
  type, 129
  under a place, 349
finitely generated
  algebra, 121
  extension, 226
  group, 66
  module, 129
  ring, 90
finitely presented, 171
Fitting ideal, 738–745
Fitting lemma, 440
five lemma, 169
fixed
  field, 261
  point, 28, 34, 80
flat, 612, 808
  for a module, 616
forgetful functor, 62
form
  multilinear, 450, 466
  polynomial, 384
formal power series, 205
Fourier coefficients, 679

fractional ideal, 88
fractions, 107
free
  abelian group, 38, 39
  extension, 362
  generators, 137
  group, 66, 82
  module, 135
  module generated by a set, 137
  resolution, 763
Frey polynomial, 198
Frobenius
  element, 180, 246, 316, 346
  reciprocity, 686, 689
functionals, 142
functor, 62
fundamental group, 63

$G$ or $(G,k)$-module, 664, 779
$G$-homomorphism, 779
$G$-object, 55
$G$-regular, 829
$G$-set, 25, 27, 55
Galois
  cohomology, 288, 302
  extension, 261
  group, 252, 262, 269
  theory, 262
Gauss lemma, 181, 209, 495
Gauss sum, 277
g.c.d., 111
Gelfand-Mazur theorem, 471
Gelfand-Naimark theorem, 406
Gelfond-Schneider, 868
generate and generators
  for a group, 9, 23, 68
  for an ideal, 87
  for a module, 660
  for a ring, 90
generating function or power series, 211
generators and relations, 68
generic
  forms, 390, 392
  hyperplane, 374
  pfaffian, 589
  point, 383, 408
  polynomial, 272, 345
ghost components, 330
$GL_2$, 300, 317, 537, 715
$GL_n$, 19, 521, 543, 546, 547
global sections, 792
Goursat's lemma, 75
graded
  algebra, 172, 631
  module, 427, 751, 765
  morphism, 765, 766
  object, 814
  ring, 631
Gram-Schmidt orthogonalization, 579, 599
Grassman algebra, 733
greatest common divisor, 111
Grothendieck
  algebra and ring, 778–782
  group, 40, 139
  power series, 218
  spectral sequence, 819
group, 7
  algebra, 104, 121
  automorphism, 10
  extensions, 827
  homomorphism, 10
  object, 65
  ring, 85, 104, 126

Hall conjecture, 197
harmonic polynomials, 354, 550
Hasse zeta function, 255
height, 167
Herbrand quotient, 79
Hermite-Lindemann, 867
hermitian
  form, 533, 571, 579
  linear map, 534
  matrix, 535
Hilbert
  Nullstellensatz, 380, 551
  polynomial, 433
  -Serre theorem, 431
  syzygy theorem, 862
  theorem on polynomial rings, 185
  theorem 90, 288
  -Zariski theorem, 409
homogeneous, 410, 427, 631
  algebraic space, 385
  ideal, 385, 436, 733
  integral closure, 409
  point, 385
  polynomial, 103, 107, 190, 384, 436
  quadratic map, 575
homology, 445, 767
  isomorphism, 767, 836
homomorphisms in categories, 765
homomorphism
  of complex, 445, 765

homomorphism (*continued*)
of groups, 10
of inverse systems, 163
of modules, 119, 122
of monoid, 10
of representations, 125
of rings, 88
homotopies of complexes, 787
Horrock's theorem, 847
Howe's proof, 258
hyperbolic
enlargement, 593
pair, 586, 590
plane, 586, 590
space, 590
hyperplane, 542
section, 374, 410

Ideal, 86
class group, 88, 126
idempotent, 443
image, 11
indecomposable, 440
independent
absolute values, 465
characters, 283, 676
elements of module, 151
extensions, 362
variables, 102, 103
index, 12
induced
character, 686
homomorphism, 16
module, 688
ordering, 879
representation, 688
inductively ordered, 880
inertia
form, 393
group, 344
infinite
cyclic group, 8, 23
cyclic module, 147
extension, 223, 235
Galois extensions, 313
period, 8, 23
set, 876
under a place, 349
infinitely
large, 450
small, 450
injective
map, ix
module, 782, 830
resolution, 788, 801, 819
inner automorphism, 26
inseparable
degree, 249
extension, 247
integers mod n, 94
integral, 334, 351, 352, 409
closure, 336, 409
domain, 91
equation, 334
extension, 340
homomorphism, 337
map, 357
root test, 185
valued polynomials, 216, 435
integrally closed, 337
integrality criterion, 352, 409
invariant
bases, 550
submodule, 665
invariant
of linear map, 557, 560
of matrix, 557
of module, 153, 557, 563
of submodule, 153, 154
inverse, ix, 7
inverse limit, 50, 51, 161, 163, 169
of Galois groups, 313, 328
inverse matrix, 518
invertible, 84
Irr($z$,$k$,$X$), 224
irreducible
algebraic set, 382, 408
character, 669, 696
element, 111
module, 554
polynomial, 175, 183
polynomial of a field element, 224
irrelevant prime, 436
isolated prime, 422
isometry, 572
isomorphism, 10, 54
of representations, 56, 667
isotropy group, 27
Iss'sa-Hironaka theorem, 498

Jacobson
density, 647
radical, 658
Jordan-Hölder, 22, 156
Jordan canonical form, 559

*K*-family, 771
*K*-theory, 139, 771–782
kernel
  of bilinear map, 48, 144, 522, 572
  of homomorphism, 11, 133
Kolchin's theorem, 661
Koszul complex, 853
Krull
  theorem, 429
  topology, 329
Krull-Remak-Schmidt, 441
Kummer extensions
  abelian, 294–296, 332
  non-abelian, 297, 304, 326

*L*-functions, 727
lambda operation, 217
lambda-ring, 218, 780
Langlands conjectures, 316, 319
lattice, 662
law of composition, 3
Lazard's theorem, 639
leading coefficient, 100
least
  common multiple, 113
  element, 879
  upper bound, 879
left
  coset, 12
  derived functor, 791
  exact, 790
  ideal, 86
  module, 117
length
  of complex, 765
  of filtration, 433
  of module, 433, 644
Lie algebra, 548
lie above
  prime, 338
  valuation ring, 350
lifting, 227
linear
  combination, 129
  dependence, 130
  independence, 129, 150, 283
  map, 119
  polynomial, 100
linearly disjoint, 360
local
  degree, 477
  homomorphism, 444
  norm, 478
  parameter, 487
  ring, 110, 425, 441
  uniformization, 498
localization, 110
locally nilpotent, 418
logarithm, 497, 597
logarithmic derivative, 214, 375

Mackey's theorems, 694
MacLane's criterion, 364
mapping cylinder, 838
Maschke's theorem, 666
Mason-Stothers theorem, 194, 220
matrix, 503
  of bilinear map, 528
  over non-commutative ring, 641
maximal
  abelian extension, 269
  archimedean, 450
  element, 879
  ideal, 92
metric linear map, 573
minimal polynomial, 556, 572
Mittag-Leffler condition, 164
modular forms, 318, 319
module, 117
  over principal ring, 146, 521
modulo an ideal, 90
Moebius inversion, 116, 254
monic, 175
monoid, 3
  algebra, 106, 126
  homomorphism, 10
monomial, 101
monomorphism, 120
Morita's theorem, 660
morphism, 53
  of complex, 765
  of functor, 65, 625, 800
  or representation, 125
multilinear map, 511, 521, 602
multiple root, 178, 247
multiplicative
  function, 116
  subgroup of a field, 177
  subset, 107
multiplicity
  of character, 670
  of root, 178
  of simple module, 644

Nakayama's lemma, 424, 661
natural transformation, 65

negative, 449
  definite, 578
Newton approximation, 493
nilpotent, 416, 559, 569
Noether normalization, 357
Noetherian, 186, 210, 408–409, 415, 427
  graded ring, 427
  module, 413
non-commutative variables, 633
non-degenerate, 522, 572
non-singular, 523, 529
norm, 284, 578, 637
  on a vector space, 469
  on a finitely generated abelian group, 166
normal
  basis theorem, 312
  endomorphism, 597
  extension, 238
  subgroup, 14
  tower, 18
normalizer, 14
Northcott theorems, 864
null
  sequence, 52
  space, 586
nullstellensatz, 380, 383

occur, 102, 176
odd permutation, 31
one-dimensional
  character, 671
  representation, 671
open complex, 761
open set, 406
operate
  on a module, 664
  on an object, 55
  on a set, 25, 76
orbit, 28
  decomposition formula, 29
order
  of a group, 12
  at $p$, 113, 488
  at a valuation, 488
  of a zero, 488
ordering, 449, 480, 878
ordinary tensor product, 630
orthogonal
  basis, 572–585
  element, 48, 144, 572
  group, 535
  map, 535
  sum, 572
orthogonality relations, 677
orthogonalization, 579
orthonormal, 577
over a map, 229

$p$-adic
  integers, 51, 162, 169, 488
  numbers, 488
$p$-class, 706
$p$-conjugate, 706
$p$-divisible, 50
$p$-elementary, 705
$p$-group, 33
$p$-regular, 705
$p$-singular, 705
$p$-subgroup, 33
pairing, 48
parallelogram law, 598
partial fractions, 187
partition, 79
  function, 211
perfect, 252
period, 23, 148
periodicity of Clifford algebra, 758
permutation, 8, 30
perpendicular, 48, 144, 522
Pfaffian, 589
Pic or Picard group, 88, 126
place, 349, 482
Poincaré series, 211, 431
point
  of algebraic set, 383
  in a field, 408
polar decomposition, 584
polarization identity, 580
pole, 488
polynomial, 97
  algebra, 97, 633
  function, 98
  invariants, 557
  irreducible, 175, 183
  Noetherian, 185
Pontrjagin dual, 145
positive, 449
  definite, 578, 583
power map, 10
power series, 205
  factorial, 209
  Noetherian, 210
primary
  decomposition, 422
  ideal, 421
  module, 421

prime
element, 113
field, 90
ideal, 92
ring, 90
primitive
element, 243, 244
group, 80
operation, 79
polynomials, 181, 182
power series, 209
root, 301
root of unity, 277, 278
principal
homomorphism, 418
ideal, 86, 88
module, 554, 556
representation, 554
ring, 86, 146, 521
product
in category, 58
of groups, 9
of modules, 127
of rings, 91
profinite, 51
projection, 388
projective
module, 137, 168, 848, 850
resolution, 763
space, 386
proper, ix
congruence, 492
pull-back, 61
purely inseparable
element, 249
extension, 250
push-out, 62, 81

quadratic
extension, 269
form, 575
map, 574
symbol, 281
quadratically closed, 462
quaternions, 9, 545, 723, 758
Quillen-Suslin theorem, 848
quotient
field, 110
ring, 107

radical
of an ideal, 388, 417
of a ring, 661
of an integer, 195
Ramanujan power series, 212
ramification index, 483
rank, 42, 46
of a matrix, 506
rational
conjugacy class, 276, 326, 725
element, 714
function, 110
real, 451
closed, 451
closure, 452
place, 462
zero, 457
reduced
decomposition, 422, 443
polynomial, 177
reduction
criterion, 185
map, 99, 102
modulo an ideal, 446, 623
mod $p$, 623
refinement of a tower, 18
regular
character, 675, 699
extension, 366
module, 699, 829
representation, 675, 829
sequence, 850
relations, 68
relative invariant, 171, 327
relatively prime, 113
representation, 55, 124, 126
functor, 64
of a group, 55, 317, 664
of a ring, 553
space, 667
residue class, 91
degree, 422, 483
ring, 91
resolution, 763, 798
resultant, 200, 398, 410
system, 403
variety, 393
Ribet, 319
Rieffel's theorem, 655
Riemann surface, 275
Riemann-Roch, 212, 218, 220, 258
right
coset, 12, 75
derived functor, 791
exact functor, 791, 798

right (*continued*)
ideal, 66
module, 117
rigid, 275
rigidity theorem, 276
ring, 83
homomorphism, 88
of fractions, 107
root, 175
of unity, 177, 276
row
operation, 154
rank, 506
vector, 503

$S_3$ and $S_4$, 722
scalar product, 571
Schanuel
conjecture, 873
lemma, 841
Schreier's theorem, 22
Schroeder-Bernstein theorem, 885
Schur
Galois groups, 274
lemma, 643
Schwarz inequality, 578, 580
section, 64, 792
self-adjoint, 581
semidirect product, 15, 76
semilinear, 532
seminorm, 166, 475
semipositive, 583, 597
semisimple
endomorphism, 569, 661
module, 554, 647, 659
representation, 554, 712
ring, 651
separable
closure, 243
degree, 239
element, 240
extension, 241, 658
polynomial, 241
separably generated, 363
separating transcendence basis, 363
sequence, 875
Serre's conjecture, 848
theorem, 844
sesquilinear form, 532
Shafarevich conjecture, 314
sheaf, 792
sign of a permutation, 31, 77
simple
character, 669
group, 20
module, 156, 554, 643
ring, 653, 655
root, 247
simplicity of $SL_n$, 539, 542
size of a matrix, 503
skew symmetric, 526
$SL_2$, 69, 537, 539, 546
generators and relations, 69, 70, 537
$SL_n$, 521, 539, 541, 547
snake lemma, 158, 169, 614–621
Snyder's proof, 220
solvable
extension, 291, 314
group, 18, 293, 314
by radicals, 292
spec of a ring, 405, 410
special linear group, 14, 52, 59, 69, 541, 546, 547
specializing, 101
specialization, 384
spectral
sequence, 815–825
theorem, 581, 583, 585
split exact sequence, 132
splitting field, 235
square
matrix, 504
group, 9, 77, 270
root of operator, 584
stably free, 840
dimension, 840
stably isomorphic, 841
stalk, 161
standard
complex, 764
alternating matrix, 587
Steinberg theorem, 726
Stewart-Tijdeman, 196
strictly inductively ordered, 881
stripping functor, 62
Sturm's theorem, 454
subgroup, 9
submodule, 118
submonoid, 6
subobject, 134
subring, 84
subsequence, 876
subspace, 141
substituting, 98, 101

super
  algebra, 632
  commutator, 757
  product, 631, 751
  tensor product, 632, 751
supersolvable, 702
support, 419
surjective, ix
Sylow group, 33
Sylvester's theorem, 577
symmetric
  algebra, 635
  endomorphism, 525, 585, 597
  form, 525, 571
  group, 28, 30, 269, 272–274
  matrix, 530
  multilinear map, 635
  polynomial, 190, 217
  product, 635, 781, 861
symplectic, 535
  basis, 599
syzygy theorem, 862
Szpiro conjecture, 198

Taniyama-Shimura conjecture, 316, 319
Tate group, 50, 163, 169
  limit, 598
Taylor series, 213
tensor, 581, 628
  algebra, 633
  exact, 612
  product, 602, 725
  product of complexes, 832, 851
  product representation, 725, 799
Tits construction of free group, 81
tor (for torsion), 42, 47, 149
Tor, 622, 791
  dimension, 622
Tornheim proof, 471
torsion
  free, 45, 147
  module, 147, 149
total
  complex, 815
  degree, 103
totally ordered, 879
tower
  of fields, 225
  of groups, 18
trace
  of element, 284, 666
  of linear map, 511, 570
  of matrix, 505, 511
transcendence
  basis, 356
  degree, 355
  of e, 867
transcendental, 99
transitive, 28, 79
translation, 26, 227
transpose
  of bifunctor, 808
  of linear map, 524
  of matrix, 505
transposition, 13
transvection, 542
trigonometric degree, 115
  polynomial, 114, 115
trivial
  character, 282
  operation, 664
  representation, 664
  subgroup, 9
  valuation, 465
two-sided ideal, 86, 655
type
  of abelian group, 43
  of module, 149

unimodular, 846
  extension property, 849
unipotent, 714
unique factorization, 111, 116
uniquely divisible, 575
unit, 84
  element, 3, 83
  ideal, 87
unitary, 535, 583
universal, 37
  delta-functor, 800
  derivation, 746
universally
  attracting, 57
  repelling, 57
upper bound, 879
upper diagonal group, 19

valuation, 465
valuation ring, 348, 481
  determined by ordering, 450, 452
value group, 480
Vandermonde determinant, 257–259, 516
vanishing ideal, 38
variable, 99, 104
variation of signs, 454

variety, 382
vector space, 118, 139
volume, 735

Warning's theorem, 214
Wedderburn's theorem, 649
Weierstrass
  degree, 208
  polynomial, 208
  preparation theorem, 208
weight, 191
well-behaved, 410, 478
well-defined, x
well-ordering, 891
Weyl group, 570
Witt group, 594, 599
  theorem, 591
  vector, 330, 492
Witt-Grothendieck group, 595

Zariski-Matsusaka theorem, 372
Zariski topology, 407
Zassenhaus lemma, 20
zero
  divisor, 91
  element, 3
  of ideal, 390, 405
  of polynomial, 102, 175, 379, 390
zeta function, 211, 212, 255
Zorn's lemma, 880, 884

# Graduate Texts in Mathematics

1 TAKEUTI/ZARING. Introduction to Axiomatic Set Theory. 2nd ed.
2 OXTOBY. Measure and Category. 2nd ed.
3 SCHAEFER. Topological Vector Spaces. 2nd ed.
4 HILTON/STAMMBACH. A Course in Homological Algebra. 2nd ed.
5 MAC LANE. Categories for the Working Mathematician. 2nd ed.
6 HUGHES/PIPER. Projective Planes.
7 J.-P. SERRE. A Course in Arithmetic.
8 TAKEUTI/ZARING. Axiomatic Set Theory.
9 HUMPHREYS. Introduction to Lie Algebras and Representation Theory.
10 COHEN. A Course in Simple Homotopy Theory.
11 CONWAY. Functions of One Complex Variable I. 2nd ed.
12 BEALS. Advanced Mathematical Analysis.
13 ANDERSON/FULLER. Rings and Categories of Modules. 2nd ed.
14 GOLUBITSKY/GUILLEMIN. Stable Mappings and Their Singularities.
15 BERBERIAN. Lectures in Functional Analysis and Operator Theory.
16 WINTER. The Structure of Fields.
17 ROSENBLATT. Random Processes. 2nd ed.
18 HALMOS. Measure Theory.
19 HALMOS. A Hilbert Space Problem Book. 2nd ed.
20 HUSEMOLLER. Fibre Bundles. 3rd ed.
21 HUMPHREYS. Linear Algebraic Groups.
22 BARNES/MACK. An Algebraic Introduction to Mathematical Logic.
23 GREUB. Linear Algebra. 4th ed.
24 HOLMES. Geometric Functional Analysis and Its Applications.
25 HEWITT/STROMBERG. Real and Abstract Analysis.
26 MANES. Algebraic Theories.
27 KELLEY. General Topology.
28 ZARISKI/SAMUEL. Commutative Algebra. Vol.I.
29 ZARISKI/SAMUEL. Commutative Algebra. Vol.II.
30 JACOBSON. Lectures in Abstract Algebra I. Basic Concepts.
31 JACOBSON. Lectures in Abstract Algebra II. Linear Algebra.
32 JACOBSON. Lectures in Abstract Algebra III. Theory of Fields and Galois Theory.
33 HIRSCH. Differential Topology.
34 SPITZER. Principles of Random Walk. 2nd ed.
35 ALEXANDER/WERMER. Several Complex Variables and Banach Algebras. 3rd ed.
36 KELLEY/NAMIOKA et al. Linear Topological Spaces.
37 MONK. Mathematical Logic.
38 GRAUERT/FRITZSCHE. Several Complex Variables.
39 ARVESON. An Invitation to $C^*$-Algebras.
40 KEMENY/SNELL/KNAPP. Denumerable Markov Chains. 2nd ed.
41 APOSTOL. Modular Functions and Dirichlet Series in Number Theory. 2nd ed.
42 J.-P. SERRE. Linear Representations of Finite Groups.
43 GILLMAN/JERISON. Rings of Continuous Functions.
44 KENDIG. Elementary Algebraic Geometry.
45 LOÈVE. Probability Theory I. 4th ed.
46 LOÈVE. Probability Theory II. 4th ed.
47 MOISE. Geometric Topology in Dimensions 2 and 3.
48 SACHS/WU. General Relativity for Mathematicians.
49 GRUENBERG/WEIR. Linear Geometry. 2nd ed.
50 EDWARDS. Fermat's Last Theorem.
51 KLINGENBERG. A Course in Differential Geometry.
52 HARTSHORNE. Algebraic Geometry.
53 MANIN. A Course in Mathematical Logic.
54 GRAVER/WATKINS. Combinatorics with Emphasis on the Theory of Graphs.
55 BROWN/PEARCY. Introduction to Operator Theory I: Elements of Functional Analysis.
56 MASSEY. Algebraic Topology: An Introduction.
57 CROWELL/FOX. Introduction to Knot Theory.
58 KOBLITZ. $p$-adic Numbers, $p$-adic Analysis, and Zeta-Functions. 2nd ed.
59 LANG. Cyclotomic Fields.
60 ARNOLD. Mathematical Methods in Classical Mechanics. 2nd ed.
61 WHITEHEAD. Elements of Homotopy Theory.
62 KARGAPOLOV/MERLZJAKOV. Fundamentals of the Theory of Groups.
63 BOLLOBAS. Graph Theory.

# Graduate Texts in Mathematics

64 EDWARDS. Fourier Series. Vol. I. 2nd ed.
65 WELLS. Differential Analysis on Complex Manifolds. 2nd ed.
66 WATERHOUSE. Introduction to Affine Group Schemes.
67 SERRE. Local Fields.
68 WEIDMANN. Linear Operators in Hilbert Spaces.
69 LANG. Cyclotomic Fields II.
70 MASSEY. Singular Homology Theory.
71 FARKAS/KRA. Riemann Surfaces. 2nd ed.
72 STILLWELL. Classical Topology and Combinatorial Group Theory. 2nd ed.
73 HUNGERFORD. Algebra.
74 DAVENPORT. Multiplicative Number Theory. 3rd ed.
75 HOCHSCHILD. Basic Theory of Algebraic Groups and Lie Algebras.
76 IITAKA. Algebraic Geometry.
77 HECKE. Lectures on the Theory of Algebraic Numbers.
78 BURRIS/SANKAPPANAVAR. A Course in Universal Algebra.
79 WALTERS. An Introduction to Ergodic Theory.
80 ROBINSON. A Course in the Theory of Groups. 2nd ed.
81 FORSTER. Lectures on Riemann Surfaces.
82 BOTT/TU. Differential Forms in Algebraic Topology.
83 WASHINGTON. Introduction to Cyclotomic Fields. 2nd ed.
84 IRELAND/ROSEN. A Classical Introduction to Modern Number Theory. 2nd ed.
85 EDWARDS. Fourier Series. Vol. II. 2nd ed.
86 VAN LINT. Introduction to Coding Theory. 2nd ed.
87 BROWN. Cohomology of Groups.
88 PIERCE. Associative Algebras.
89 LANG. Introduction to Algebraic and Abelian Functions. 2nd ed.
90 BRØNDSTED. An Introduction to Convex Polytopes.
91 BEARDON. On the Geometry of Discrete Groups.
92 DIESTEL. Sequences and Series in Banach Spaces.
93 DUBROVIN/FOMENKO/NOVIKOV. Modern Geometry—Methods and Applications. Part I. 2nd ed.
94 WARNER. Foundations of Differentiable Manifolds and Lie Groups.
95 SHIRYAEV. Probability. 2nd ed.
96 CONWAY. A Course in Functional Analysis. 2nd ed.
97 KOBLITZ. Introduction to Elliptic Curves and Modular Forms. 2nd ed.
98 BRÖCKER/TOM DIECK. Representations of Compact Lie Groups.
99 GROVE/BENSON. Finite Reflection Groups. 2nd ed.
100 BERG/CHRISTENSEN/RESSEL. Harmonic Analysis on Semigroups: Theory of Positive Definite and Related Functions.
101 EDWARDS. Galois Theory.
102 VARADARAJAN. Lie Groups, Lie Algebras and Their Representations.
103 LANG. Complex Analysis. 3rd ed.
104 DUBROVIN/FOMENKO/NOVIKOV. Modern Geometry—Methods and Applications. Part II.
105 LANG. $SL_2(\mathbf{R})$.
106 SILVERMAN. The Arithmetic of Elliptic Curves.
107 OLVER. Applications of Lie Groups to Differential Equations. 2nd ed.
108 RANGE. Holomorphic Functions and Integral Representations in Several Complex Variables.
109 LEHTO. Univalent Functions and Teichmüller Spaces.
110 LANG. Algebraic Number Theory.
111 HUSEMÖLLER. Elliptic Curves. 2nd ed.
112 LANG. Elliptic Functions.
113 KARATZAS/SHREVE. Brownian Motion and Stochastic Calculus. 2nd ed.
114 KOBLITZ. A Course in Number Theory and Cryptography. 2nd ed.
115 BERGER/GOSTIAUX. Differential Geometry: Manifolds, Curves, and Surfaces.
116 KELLEY/SRINIVASAN. Measure and Integral. Vol. I.
117 J.-P. SERRE. Algebraic Groups and Class Fields.
118 PEDERSEN. Analysis Now.
119 ROTMAN. An Introduction to Algebraic Topology.
120 ZIEMER. Weakly Differentiable Functions: Sobolev Spaces and Functions of Bounded Variation.
121 LANG. Cyclotomic Fields I and II. Combined 2nd ed.
122 REMMERT. Theory of Complex Functions. *Readings in Mathematics*
123 EBBINGHAUS/HERMES et al. Numbers. *Readings in Mathematics*

124 DUBROVIN/FOMENKO/NOVIKOV. Modern Geometry—Methods and Applications. Part III
125 BERENSTEIN/GAY. Complex Variables: An Introduction.
126 BOREL. Linear Algebraic Groups. 2nd ed.
127 MASSEY. A Basic Course in Algebraic Topology.
128 RAUCH. Partial Differential Equations.
129 FULTON/HARRIS. Representation Theory: A First Course.
*Readings in Mathematics*
130 DODSON/POSTON. Tensor Geometry.
131 LAM. A First Course in Noncommutative Rings. 2nd ed.
132 BEARDON. Iteration of Rational Functions.
133 HARRIS. Algebraic Geometry: A First Course.
134 ROMAN. Coding and Information Theory.
135 ROMAN. Advanced Linear Algebra.
136 ADKINS/WEINTRAUB. Algebra: An Approach via Module Theory.
137 AXLER/BOURDON/RAMEY. Harmonic Function Theory. 2nd ed.
138 COHEN. A Course in Computational Algebraic Number Theory.
139 BREDON. Topology and Geometry.
140 AUBIN. Optima and Equilibria. An Introduction to Nonlinear Analysis.
141 BECKER/WEISPFENNING/KREDEL. Gröbner Bases. A Computational Approach to Commutative Algebra.
142 LANG. Real and Functional Analysis. 3rd ed.
143 DOOB. Measure Theory.
144 DENNIS/FARB. Noncommutative Algebra.
145 VICK. Homology Theory. An Introduction to Algebraic Topology. 2nd ed.
146 BRIDGES. Computability: A Mathematical Sketchbook.
147 ROSENBERG. Algebraic $K$-Theory and Its Applications.
148 ROTMAN. An Introduction to the Theory of Groups. 4th ed.
149 RATCLIFFE. Foundations of Hyperbolic Manifolds.
150 EISENBUD. Commutative Algebra with a View Toward Algebraic Geometry.
151 SILVERMAN. Advanced Topics in the Arithmetic of Elliptic Curves.
152 ZIEGLER. Lectures on Polytopes.
153 FULTON. Algebraic Topology: A First Course.
154 BROWN/PEARCY. An Introduction to Analysis.
155 KASSEL. Quantum Groups.
156 KECHRIS. Classical Descriptive Set Theory.
157 MALLIAVIN. Integration and Probability.
158 ROMAN. Field Theory.
159 CONWAY. Functions of One Complex Variable II.
160 LANG. Differential and Riemannian Manifolds.
161 BORWEIN/ERDÉLYI. Polynomials and Polynomial Inequalities.
162 ALPERIN/BELL. Groups and Representations.
163 DIXON/MORTIMER. Permutation Groups.
164 NATHANSON. Additive Number Theory: The Classical Bases.
165 NATHANSON. Additive Number Theory: Inverse Problems and the Geometry of Sumsets.
166 SHARPE. Differential Geometry: Cartan's Generalization of Klein's Erlangen Program.
167 MORANDI. Field and Galois Theory.
168 EWALD. Combinatorial Convexity and Algebraic Geometry.
169 BHATIA. Matrix Analysis.
170 BREDON. Sheaf Theory. 2nd ed.
171 PETERSEN. Riemannian Geometry.
172 REMMERT. Classical Topics in Complex Function Theory.
173 DIESTEL. Graph Theory. 2nd ed.
174 BRIDGES. Foundations of Real and Abstract Analysis.
175 LICKORISH. An Introduction to Knot Theory.
176 LEE. Riemannian Manifolds.
177 NEWMAN. Analytic Number Theory.
178 CLARKE/LEDYAEV/STERN/WOLENSKI. Nonsmooth Analysis and Control Theory.
179 DOUGLAS. Banach Algebra Techniques in Operator Theory. 2nd ed.
180 SRIVASTAVA. A Course on Borel Sets.
181 KRESS. Numerical Analysis.
182 WALTER. Ordinary Differential Equations.

183 MEGGINSON. An Introduction to Banach Space Theory.
184 BOLLOBAS. Modern Graph Theory.
185 COX/LITTLE/O'SHEA. Using Algebraic Geometry.
186 RAMAKRISHNAN/VALENZA. Fourier Analysis on Number Fields.
187 HARRIS/MORRISON. Moduli of Curves.
188 GOLDBLATT. Lectures on the Hyperreals: An Introduction to Nonstandard Analysis.
189 LAM. Lectures on Modules and Rings.
190 ESMONDE/MURTY. Problems in Algebraic Number Theory.
191 LANG. Fundamentals of Differential Geometry.
192 HIRSCH/LACOMBE. Elements of Functional Analysis.
193 COHEN. Advanced Topics in Computational Number Theory.
194 ENGEL/NAGEL. One-Parameter Semigroups for Linear Evolution Equations.
195 NATHANSON. Elementary Methods in Number Theory.
196 OSBORNE. Basic Homological Algebra.
197 EISENBUD/HARRIS. The Geometry of Schemes.
198 ROBERT. A Course in $p$-adic Analysis.
199 HEDENMALM/KORENBLUM/ZHU. Theory of Bergman Spaces.
200 BAO/CHERN/SHEN. An Introduction to Riemann–Finsler Geometry.
201 HINDRY/SILVERMAN. Diophantine Geometry: An Introduction.
202 LEE. Introduction to Topological Manifolds.
203 SAGAN. The Symmetric Group: Representations, Combinatorial Algorithms, and Symmetric Functions.
204 ESCOFIER. Galois Theory.
205 FÉLIX/HALPERIN/THOMAS. Rational Homotopy Theory. 2nd ed.
206 MURTY. Problems in Analytic Number Theory.
*Readings in Mathematics*
207 GODSIL/ROYLE. Algebraic Graph Theory.
208 CHENEY. Analysis for Applied Mathematics.
209 ARVESON. A Short Course on Spectral Theory.
210 ROSEN. Number Theory in Function Fields.
211 LANG. Algebra. Revised 3rd ed.
212 MATOUŠEK. Lectures on Discrete Geometry.
213 FRITZSCHE/GRAUERT. From Holomorphic Functions to Complex Manifolds.
214 JOST. Partial Differential Equations.
215 GOLDSCHMIDT. Algebraic Functions and Projective Curves.
216 D. SERRE. Matrices: Theory and Applications.
217 MARKER. Model Theory: An Introduction.
218 LEE. Introduction to Smooth Manifolds.
219 MACLACHLAN/REID. The Arithmetic of Hyperbolic 3-Manifolds.
220 NESTRUEV. Smooth Manifolds and Observables.
221 GRÜNBAUM. Convex Polytopes. 2nd ed.
222 HALL. Lie Groups, Lie Algebras, and Representations: An Elementary Introduction.
223 VRETBLAD. Fourier Analysis and Its Applications.
224 WALSCHAP. Metric Structures in Differential Geometry.