Appendix A
Set Theory

In this Appendix, we will survey some of the elementary results from set theory that we use in the text. We give very few proofs and refer the reader to set theory texts such as [26], [47], or [57] for further details.

We will work in ZFC, Zermelo–Fraenkel set theory with the Axiom of Choice. The Axiom of Choice asserts that if $(A_i : i \in I)$ is a family of nonempty sets, then there is a function f with domain I such that $f(i) \in A_i$ for all $i \in I$.

Zorn's Lemma and Well-Orderings

If X is a set and $<$ is a binary relation on X, we say that $(X, <)$ is a *partial order* if $(X, <) \models \forall x\, \neg(x < x)$ and $(X, <) \models \forall x \forall y \forall z\, ((x < y \wedge y < z) \rightarrow x < z)$.

We say that $(X, <)$ is a *linear order* if in addition $(X, <) \models \forall x \forall y\, (x < y \vee x = y \vee y < x)$.

If $(X, <)$ is a partial order, then we say that $C \subseteq X$ is a *chain* in X if C is linearly ordered by $<$.

Theorem A.1 (Zorn's Lemma) *If $(X, <)$ is a partial order such that for every chain $C \subseteq X$ there is $x \in X$ such that $c \leq x$ for all $c \in C$, then there is $y \in X$ such that there is no $z \in X$ with $z > x$. In other words, if every chain has an upper bound, then there is a maximal element of X.*

We give one application of Zorn's Lemma. We say that a linear order $(A, <)$ is a *well-order* if for any nonempty $C \subseteq A$, there is $a \in C$ such that $a \leq b$ for all $b \in C$. The following characterization is also useful.

Lemma A.2 *$(A, <)$ is a well-order if and only if there is no infinite descending chain $a_0 > a_1 > a_2 > \ldots$ in A.*

Theorem A.3 (Well-Ordering Principle) *If A is any set, then there is a well-ordering of A.*

Proof Let $X = \{(Y, R) : Y \subseteq A$ and R is a well-ordering of $A\}$. We say that $(Y, R) < (Y_1, R_1)$ if $Y \subset Y_1$, $R \subset R_1$, and if $a \in Y_1 \setminus Y$ and $b \in Y$; then bRa (i.e. every new element is greater than every old element). Suppose that $C \subset X$ is a chain. Let

$$\widehat{Y} = \bigcup_{(Y,R)\in C} Y \text{ and } \widehat{R} = \bigcup_{(Y,R)\in C} R.$$

We claim that $\widehat{R}$ is a well-ordering of $\widehat{Y}$. We first show that $\widehat{R}$ is a linear order. Clearly, $\neg(a\widehat{R}a)$ for all $a \in \widehat{Y}$. If $a_1, a_2, a_3 \in \widehat{Y}$ such that $a_1\widehat{R}a_2$ and $a_2\widehat{R}a_3$, then we can find $(Y_i, R_i) \in C$ such that $a_i \in Y_i$ for $i = 1, 2, 3$. Because C is a chain, there is j such that $(Y_i, R_i) \leq (Y_j, R_j)$ for each $i = 1, 2, 3$. Because (Y_i, R_i) is transitive, $a_1 R_j a_3$ and $a_1 \widehat{R} a_3$.

If $a_0 > a_1 > \ldots$ is a decreasing chain in $\widehat{R}$, we can find $(Y, R) \in C$ such that $a_0 \in Y$. Because of the way we order X, all of the $a_i \in Y$. In this case, R would not be a well-order, a contradiction. Thus $(\widehat{Y}, \widehat{R}) \in X$. Clearly, $(\widehat{Y}, \widehat{R}) \geq (Y, R)$ for all $(Y, R) \in C$. Thus, every chain has an upper bound.

By Zorn's Lemma, there is $(Y, R) \in X$ maximal. We claim that $Y = A$. Suppose that $a \in A \setminus Y$. Let $Y' = A \cup \{a\}$, and let $R' = R \cup (Y \times \{a\})$ (i.e., we order Y' by making a the largest element). Then, R' is a well-ordering and we have contradicted the maximality of (Y, R). Thus ,R is a well-ordering of A.

Zorn's Lemma and the Well-Ordering Principle are equivalent forms of the Axiom of Choice.

Ordinals

Definition A.4 We say that X is *transitive* if, whenever $x \in X$ and $y \in x$, then $y \in X$. We say that a set X is an *ordinal* if X is transitive and well-ordered by $\in$. Let On be the class of all ordinals.

Lemma A.5 *i) On is transitive and well-ordered by $\in$.*

ii) If α and β are ordinals, then the orderings $(\alpha, \in)$ and $(\beta, \in)$ are isomorphic if and only if $\alpha = \beta$.

It follows from i) that On is not a set. If On were a set, then On is itself an ordinal and $On \in On$. This gives rise to an infinite descending chain contradicting the fact that On is well-ordered by $\in$.

Because $\in$ is an ordering of On we often write $\alpha < \beta$ instead of $\alpha \in \beta$. Note that $\alpha = \{\beta \in On : \beta < \alpha\}$.

Every well-ordering is isomorphic to an ordinal.

Proposition A.6 *If $(X, <)$ is a well-ordering, then there is an ordinal α such that $(X, <)$ is isomorphic to $(\alpha, \in)$. We call α the* order type *of $(X, <)$.*

Lemma A.7 *i) $\emptyset$ is an ordinal and if $\alpha \in On$, and $\alpha \neq \emptyset$ then $\emptyset \in \alpha$. Thus, $\emptyset$ is the least ordinal.*

ii) If α is an ordinal, then $\mathrm{suc}(\alpha) = \alpha \cup \{\alpha\}$ is an ordinal, and if $\beta \in On$, then $\beta \leq \alpha$ or $suc(\alpha) \leq \beta$.

iii) If C is a set of ordinals, then $\delta = \bigcup_{\alpha\in C} \alpha$ is an ordinal, and δ is the least upper bound of the ordinals in C.

Lemma A.7 gives us a description of the first ordinals. By i), $0 = \emptyset$ is the least ordinal. The next ordinals are $1 = \{\emptyset\}$, $2 = \{\emptyset, \{\emptyset\}\}, \ldots$. In general, we let $n + 1 = \mathrm{suc}(n)$. Note that $n = \{0, 1, \ldots, n - 1\}$. Thus, the natural numbers are an initial segment of the ordinals. The next ordinal is $\omega = \{0, 1, 2, 3, \ldots\}$.

If $\alpha \in On$, we say that α is a *successor ordinal* if $\alpha = \mathrm{suc}(\beta)$ for some ordinal β. If $\alpha \neq 0$ and α is not a successor ordinal then we can say α is a *limit ordinal*. The next proposition is the main tool for proving things about ordinals.

Theorem A.8 (Transfinite Induction) *Suppose that C is a subclass of the ordinals such that*

i) $0 \in C$,

ii) if $\alpha \in C$, then $suc(\alpha) \in C$, and

iii) if α is a limit ordinal and $\beta \in C$ for all $\beta < \alpha$, then $\alpha \in C$.

Then $C = On$.

We can define addition, multiplication, and exponentiation of ordinals. If $\alpha, \beta \in On$, let X be the well-order obtained by putting a copy of β after a copy of α. More precisely, $X = (\{0\} \times \alpha) \cup (\{1\} \times \beta)$ with the lexicographic order. Then $\alpha + \beta$ is the order type of X. Let Y be the well-order obtained by taking the lexicographic order on $\beta \times \alpha$. Then $\alpha \cdot \beta$ is the order type of $\beta \times \alpha$. We define α^β by transfinite recursion as follows:

i) $\alpha^0 = 1$;

ii) $\alpha^{\mathrm{suc}(\beta)} = \alpha^\beta \alpha$;

iii) if β is a limit ordinal, then $\alpha^\beta = \sup\{\alpha^\gamma : \gamma < \beta\} = \bigcup_{\gamma<\beta} \alpha^\gamma$.

Addition and multiplication are not commutative, but we do have the following properties.

Lemma A.9 *i)* $\mathrm{suc}(\alpha) = \alpha + 1$.
ii) $\mathrm{suc}(\alpha + \beta) = \alpha + \mathrm{suc}(\beta)$.
iii) $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$.
iv) $\alpha(\beta\gamma) = (\alpha\beta)\gamma$.
v) $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$.
vi) If $\beta = \sup_{\gamma \in C} \gamma$, *then* $\alpha + \beta = \sup_{\gamma \in C} \alpha + \gamma$.

We can start building the ordinals above ω:
$\omega, \omega+1, \omega+2, \ldots$, $\sup\{\omega + n : n < \omega\} = \omega + \omega = \omega 2$, $\omega 2 + 1, \omega 2 + 2, \ldots$, $\sup\{\omega 2 + n : n < \omega\} = \omega 2 + \omega = \omega 3$, $\ldots, \omega 3, \ldots, \omega 4, \ldots, \omega 5 \ldots$, $\sup\{\omega n : n < \omega\} = \omega \times \omega = \omega^2$, $\omega^2 + 1, \ldots, \omega^3, \ldots, \omega^4, \ldots$, $\sup\{\omega^n : n < \omega\} = \omega^\omega$.
Continuing this way: $\ldots, \omega^{\omega+1}, \ldots, \omega^{\omega+2}, \ldots, \omega^{\omega 2}, \ldots, \omega^{\omega 3}, \ldots, \omega^{\omega^2}, \ldots, \omega^{\omega^n}, \ldots, \omega^{\omega^\omega}, \ldots, \omega^{\omega^{\omega^\omega}}, \ldots$

This is the limit of the ordinals we can easily describe. The next ordinal is

$$\epsilon_0 = \sup\{\omega, \omega^\omega, \omega^{\omega^\omega}, \ldots\}.$$

We could now continue as before. Indeed, all of the ordinals we have described so far are still quite small.

Cardinals

We need a method of comparing sizes of sets. Let A be any set. By the Well-Ordering Principle, there is a well-ordering $<$ of A and, by Proposition A.6, there is an ordinal α such that $(A, <)$ is isomorphic to α. We let $|A|$ be the least ordinal α such that there is a well-ordering of A isomorphic to α.

Proposition A.10 *The following are equivalent.*
i) $|A| = |B|$.
ii) There is a bijection $f : A \to B$.
iii) There are one-to-one functions $f : A \to B$ *and* $g : B \to A$.

We say that A is *countable* if $|A| \leq \omega$. All of the ordinals $\alpha \leq \epsilon_0$ that we described above are countable. Let $\omega_1 = \{\alpha \in On : \alpha \text{ is countable}\}$. It is easy to see that ω_1 is transitive and well-ordered by $\in$. If ω_1 is countable, then $\omega_1 \in \omega_1$ and we get a contradiction. Thus, ω_1 is the first uncountable ordinal. Note that $|\omega_1| = \omega_1$.

We say that an ordinal α is a *cardinal* if $|\alpha| = \alpha$. We recursively define ω_α for $\alpha \in On$ as follows:
$\omega_0 = \omega$;
$\omega_{\alpha+1} = \{\delta \in On : |\delta| = \omega_\alpha\}$;
if α is a limit ordinal, then $\omega_\alpha = \sup_{\beta < \alpha} \omega_\beta$.

Proposition A.11 *i) Each* ω_α *is a cardinal and* $\omega_\alpha < \omega_\beta$ *if* $\alpha < \beta$.
ii) If κ *is a cardinal, then either* $\kappa < \omega$ *or* $\kappa = \omega_\alpha$ *for some* $\alpha \in On$.

We also use the notation $\aleph_\alpha = \omega_\alpha$. When we are thinking of it as an ordinal, we use ω_α and when we are thinking of it as a cardinal, we use $\aleph_\alpha$.

If κ is a cardinal, there is a least cardinal greater than κ, which we call κ^+. We say that κ is a *successor cardinal* if $\kappa = \lambda^+$ for some λ, otherwise (if κ is nonzero), we say that κ is a *limit cardinal*. Note that infinite successor cardinals are limit ordinals.

For any limit ordinal $\alpha \geq \omega$, the *cofinality* of α is the least cardinal λ such that there is a function $f : \lambda \to \alpha$ and the image of f is unbounded in α. We let $\mathrm{cof}(\alpha)$ denote the cofinality of α.

For example, $\mathrm{cof}(\omega) = \aleph_0$ because a finite function cannot be unbounded in ω. On the other hand, $\mathrm{cof}(\omega_\omega) = \omega$ because the function $n \mapsto \omega_n$ has unbounded image.

If $\kappa \geq \aleph_0$ is a cardinal, we say that κ is *regular* if $\mathrm{cof}(\kappa) = \kappa$; otherwise, we say that κ is *singular*.

Proposition A.12 *If* $\kappa \geq \aleph_0$ *is a cardinal, then* κ^+ *is regular.*

$\aleph_0$ is a regular limit cardinal. It may be the only cardinal with both properties. We say that $\kappa > \aleph_0$ is *inaccessible* if κ is a regular limit cardinal. Although we cannot prove that inaccessible cardinals exist, it seems likely that we also cannot prove that they do not exist. Inaccessible cardinals are quite large.

Proposition A.13 *If* $\kappa > \aleph_0$ *is inaccessible, then* $\kappa = \aleph_\kappa$.

Proof An induction shows that $\omega_\alpha \geq \alpha$ for all α. If $\kappa = \aleph_\alpha$ where $\alpha < \kappa$, then $\beta \mapsto \omega_\beta$ is an unbounded map from α into κ, a contradiction.

Cardinal Arithmetic

We define addition and multiplication of cardinals. If $|X| = \kappa$ and $|Y| = \lambda$, then $\kappa + \lambda = |(\{0\} \times X) \cup (\{1\} \times Y)|$ and $\kappa\lambda = |X \times Y|$. These operations are commutative but not very interesting.

Lemma A.14 *Let* κ *and* λ *be cardinals. If* κ *and* λ *are both finite, then these operations agree with the usual arithmetic operations. If either* κ *or* λ *is infinite, then*

$$\kappa + \lambda = \kappa\lambda = \max\{\kappa, \lambda\}.$$

Corollary A.15 *i) If* $|I| = \kappa$ *and* $|A_i| \leq \kappa$ *for all* $i \in I$, *then* $|\bigcup A_i| \leq \kappa$.
ii) If κ *is regular,* $|I| < \kappa$, *and* $|A_i| < \kappa$ *for all* $i \in I$, *then* $|\bigcup A_i| < \kappa$.
iii) Let κ *be an infinite cardinal. Let* X *be a set and* $\mathcal{F}$ *a set of functions* $f : X^{n_f} \to X$. *Suppose that* $|\mathcal{F}| \leq \kappa$ *and* $A \subseteq X$ *with* $|A| \leq \kappa$. *Let* $cl(A)$ *be the smallest subset of* X *containing* A *closed under the functions in* $\mathcal{F}$. *Then* $|cl(A)| \leq \kappa$.

Exponentiation is much more interesting. If A and B are sets, then A^B is the set of functions from A to B and $|A|^{|B|} = |A^B|$.

Lemma A.16 *Let κ, λ, and μ be cardinals.*
i) $(\kappa^\lambda)^\mu = \kappa^{\lambda\mu}$.
ii) If $\lambda \geq \aleph_0$ and $2 \leq \kappa < \lambda$, then $2^\lambda = \kappa^\lambda = \lambda^\lambda$.
iii) If κ is regular and $\lambda < \kappa$, then $\kappa^\lambda = \sup\{\kappa, \mu^\lambda : \mu < \kappa\}$.

Proof iii) If $f : \lambda \to \kappa$, then, because κ is regular, there is $\alpha < \kappa$ such that $f : \lambda \to \alpha$. Thus $\kappa^\lambda = \bigcup_{\alpha<\kappa} \alpha^\lambda$. The right-hand side is the union of κ sets each of size μ^λ for some $\mu < \kappa$.

We say that an inaccessible cardinal κ is *strongly inaccessible* if $2^\lambda < \kappa$ for all $\lambda < \kappa$.

Corollary A.17 *If κ is strongly inaccessible and $\lambda < \kappa$, then $\kappa^\lambda = \kappa$.*

We know by Cantor that $2^\kappa > \kappa$ for all cardinals κ. The next theorem is a slight generalization.

Proposition A.18 (König's Theorem) *If $\kappa \geq \aleph_0$, then $\kappa^{\mathrm{cof}(\kappa)} > \kappa$.*

This gives us Cantor's theorem because $2^\kappa = \kappa^\kappa > \kappa$ but also gives us, for example, that $\aleph_\omega^{\aleph_0} > \aleph_\omega$.

ZFC is too weak to answer basic questions about cardinal exponentiation. The most interesting is the Continuum Hypothesis.

Continuum Hypothesis (CH) $2^{\aleph_0} = \aleph_1$.

Generalized Continuum Hypothesis (GCH) $2^{\aleph_\alpha} = \aleph_{\alpha+1}$.

The Continuum Hypothesis is unprovable in ZFC, but GCH is consistent with ZFC.[1] Assuming the Generalized Continuum Hypothesis, we get a complete picture of cardinal exponentiation.

Proposition A.19 *Assume the Generalized Continuum Hypothesis. Let $\kappa, \lambda \geq 2$ with at least one infinite.*
i) If $\lambda \leq \kappa$, then $\lambda^\kappa = \kappa^+$.
ii) If $\lambda < \mathrm{cof}(\kappa)$, then $\kappa^\lambda = \kappa$.
iii) If $\mathrm{cof}(\kappa) \leq \lambda < \kappa$, then $\kappa^\lambda = \kappa^+$.

Finite Branching Trees

Definition A.20 A *finite branching tree* is a partial order $(T, <)$ such that:
i) there is $r \in T$ such that $r \leq x$ for all $x \in T$;
ii) if $x \in T$, then $\{y : y < x\}$ is finite and linearly ordered by $<$;

[1] Provided ZFC itself is consistent.

iii) if $x \in T$, then there is a finite (possibly empty) set $\{y_1, \ldots, y_m\}$ of incomparable elements such that each $y_i > x$ and, if $z > x$, then $z \geq y_i$ for some i.

A *path* through T is a function $f : \omega \to T$ such that $f(n) < f(n+1)$ for all n.

Lemma A.21 (König's Lemma) *If T is an infinite finite branching tree, then there is a path through T.*

Proof Let $S(x) = \{y : y \geq x\}$ for $x \in T$. We inductively define $f(n)$ such that $S(f(n))$ is infinite for all n. Let r be the minimal element of T, then $S(r)$ is infinite. Let $f(0) = r$. Given $f(n)$, let $\{y_1, \ldots, y_m\}$ be the immediate successors of $f(n)$. Because $S(f(n)) = S(y_1) \cup \ldots \cup S(y_n)$, $S(y_i)$ is infinite for some i. Let $f(n+1) = y_i$.

Forcing Constructions

Definition A.22 Let $(P, <)$ be a partial order. We say that $F \subseteq P$ is a *filter* if:
i) if $p \in F$, $q \in P$, and $p < q$, then $q \in F$;
ii) if $p, q \in F$, there is $r \in F$ such that $r \leq p$ and $r \leq q$.
We say that $D \subseteq P$ is *dense* if for all $p \in P$ there is $q \in D$ such that $q \leq p$. If $\mathcal{D}$ is a collection of dense subsets of P, we say that $G \subseteq P$ is a *$\mathcal{D}$-generic* filter if $D \cap G \neq \emptyset$ for all $D \in \mathcal{D}$.

Lemma A.23 *For any partial order P, if $\mathcal{D}$ is a countable collection of dense subsets of P, then there is a $\mathcal{D}$-generic filter G.*

Proof Let $D_0, D_1, \ldots,$ list $\mathcal{D}$. Choose $p_0 \in P$. Given p_n, we can find $p_{n+1} \leq p_n$ with $p_{n+1} \in D_n$. Let $G = \{q : q \geq p_n \text{ for some } n\}$.

Lemma A.23 is the best we can do without extra assumptions. Let P be the set of all finite sequences of zeros and ones ordered by $p < q$ if $p \supset q$. The following sets are dense:
$E_n = \{p \in P : n \in \mathrm{dom}(p)\}$ for $n \in \omega$;
$D_f = \{p \in P : \exists n \in \mathrm{dom}(p)\ p(n) \neq f(n)\}$ for $f \in 2^\omega$.
If G is a filter meeting all of the E_n then $g = \bigcup_{p \in G} p$. Then $g : \omega \to 2$. If G meets D_f, then $g \neq f$. Thus if $\mathcal{D} = \{E_n, D_f : n \in \omega, f \in 2^\omega\}$, then there is no $\mathcal{D}$-generic filter.

We say that p and $q \in P$ are *compatible* if there is $r \leq p, q$ and say that $(P, <)$ satisfies the *countable chain condition* if whenever $A \subset P$ and any two elements of A are incompatible, then $|A| \leq \aleph_0$.

Martin's Axiom If $(P, <)$ is a partial order satisfying the countable chain condition, and $\mathcal{D}$ is a collection of dense subsets of P with $|\mathcal{D}| < 2^{\aleph_0}$, then there is a $\mathcal{D}$-generic filter on P.

Of course, if the Continuum Hypothesis is true, then Martin's Axiom is a trivial consequence of Lemma A.23. On the other hand, Martin's Axiom is consistent with, but not provable from, ZFC $+\neg$CH.

Appendix B
Real Algebra

We prove some of the algebraic facts needed in Section 3.3. All of these results are due to Artin and Schreier. See [58] XI for more details. All fields are assumed to be of characteristic 0.

Definition B.1 A field K is *real* if -1 can not be expressed as a sum of squares of elements of K. In general, we let $\sum K^2$ be the sums of squares from K.

If F is orderable, then F is real because squares are nonnegative with respect to any ordering.

Lemma B.2 *Suppose that F is real and $a \in F \setminus \{0\}$. Then, at most one of a and $-a$ is a sum of squares.*

Proof If a and b are both sums of squares, then $\frac{a}{b} = \frac{a}{b^2}b$ is a sum of squares. Thus, if F is real, at least one of a and $-a$ is not in $\sum F^2$.

Lemma B.3 *If F is real and $-a \in F \setminus \sum F^2$, then $F(\sqrt{a})$ is real. Thus, if F is real and $a \in F$, then $F(\sqrt{a})$ is real or $F(\sqrt{-a})$ is real.*

Proof We may assume that $\sqrt{a} \notin F$. If $F(\sqrt{a})$ is not real, then there are $b_i, c_i \in F$ such that

$$-1 = \sum (b_i + c_i\sqrt{a})^2 = \sum (b_i^2 + 2c_i b_i \sqrt{a} + c_i^2 a).$$

Because $\sqrt{a}$ and 1 are a vector space basis for $F(\sqrt{a})$ over F,

$$-1 = \sum b_i^2 + a \sum c_i^2.$$