Appendix D1

The Nullstellensatz and Selberg's lemma

This book is about hyperbolic manifolds and Kleinian groups: discrete subgroups of $\operatorname{Aut}\mathbb{H}^3$. Kleinian groups may have torsion, and the quotient of $\mathbb{H}^3$ by such a group is an orbifold, not a manifold.

Many people (I am among them) find it much easier to think about manifolds, even if the extra difficulties involving orbifolds are sometimes more psychological than real. Invoking *Selberg's lemma* often allows us to replace orbifolds by manifolds at no cost.

Selberg's lemma is not really a theorem in hyperbolic geometry; it is a result about finitely generated subgroups of $\mathrm{PSL}_2\,\mathbb{C}$ (and of many other algebraic groups), and never mentions discreteness. But it does involve commutative algebra, more specifically several incarnations of the *Hilbert Nullstellensatz*. Most of this appendix concerns these results.

The Hilbert Nullstellensatz is part of a standard course in commutative algebra, though deriving the variants we will require from the standard treatment might take as long as developing the subject from scratch, as we do here.

Section D1.1 is a refresher on commutative algebra, Section D1.2 introduces Jacobson rings, Section D1.3 proves several variants of the Nullstellensatz, and Section D1.4 proves Selberg's lemma.

While writing this appendix, we benefited from conversations with Ken Brown and from lecture notes he dug up from a course taught by Steven Kleiman at MIT around 1970. The presentation is also quite close to the one in Eisenbud's book [24].

D1.1 Commutative algebra: a crash course

For those readers who, like the author, find that their commutative algebra is a bit rusty and could use a spot of oil, we recall in this first section some useful generalities.

All rings will be commutative with unit, and all ring homomorphisms will map the unit element to the unit element. A ring where $ab = 0$ implies that either $a = 0$ or $b = 0$ or both is called an *integral domain*. We will call an integral domain simply a *domain*, to avoid confusion with other meanings of "integral".

Let A be a ring. An *ideal* $I \subset A$ is a subset that is a group under addition, and that is closed under multiplication by elements of A (not just by elements of I). You could also say that it is a subset of A which, with the operations of A, is an A-module. With our definition rings have units, so an ideal $I \subset A$ is usually not a ring: if it contains the unit of A it is A. If A is a ring and $I \subset A$ is an ideal, then the quotient A/I (the set of cosets of I, right or left) is naturally a ring.

An ideal is

- *proper* if it is not all of A, or, equivalently, if it does not contain 1;
- *prime* if it is proper and $ab \in I$ implies $a \in I$ or $b \in I$ or both;
- *maximal* if it is maximal among proper ideals ordered by inclusion.

If $f : A \to B$ is a ring homomorphism, then an element $b \in B$ is *integral over* A if it satisfies the equation

$$b^n + f(a_{n-1})b^{n-1} + \cdots + f(a_0) = 0 \qquad \text{D1.1.1}$$

for some choice of elements $a_0, \dots, a_{n-1}$ of A. (The key requirement here is that the polynomial be monic.) If all elements of B are integral over A, then B is integral over A.

A domain A has a *field of fractions* K_A, constructed just as the rationals are constructed from the integers. If $b \in A$ with $b \neq 0$, then $A[1/b]$ is the smallest sub-ring of K_A containing A and $1/b$. For instance, $\mathbb{Z}[1/2]$ is the ring of rational numbers with only powers of 2 in the denominator.

Of course if b is invertible in A, then $1/b$ is in A, so $A[1/b] = A$.

Some useful generalities for those who need a spot of oil

1. A proper ideal $I \subset A$ is prime if and only if A/I is a domain. An ideal $I \subset A$ is maximal if and only if A/I is a field. In particular, a maximal ideal is prime.
2. The union of any increasing family of proper ideals is a proper ideal; this and Zorn's lemma show that every proper ideal is contained in a maximal ideal.
3. A ring A is a domain if and only if the ideal $\{0\} \subset A$ is prime.
4. If $f : A \to B$ is a ring homomorphism and $P \subset B$ is a prime ideal, then $f^{-1}(P)$ is a prime ideal of A.
5. If $f : A \to B$ is a surjective ring homomorphism and M is a maximal ideal of B, then $f^{-1}(M)$ is a maximal ideal of A. If M is a maximal ideal of A containing $\ker f$, then $f(M)$ is maximal in B.
6. If an inclusion $A \subset B$ of domains makes B integral over A, then A is a field if and only if B is a field.
7. Let $A \subset B$ be an inclusion of rings, and let $x \in B$ be integral over A. Then all elements of $A[x]$ are integral over A.

The last two statements require proof.