Appendix D4
Arithmetic Kleinian groups

In this appendix we present more examples of arithmetic Kleinian groups, which will come in three flavors, discussed in Sections D4.2–D4.4:

1. the Bianchi group associated to $\mathbb{Q}(\sqrt{-5})$, illustrating the role of the *ideal class group* of a number field, and how it relates to the geometry of fundamental domains
2. an arithmetic Kleinian group Γ with $\mathbb{H}^3/\Gamma$ compact, coming from a quadratic form (this is an analogue of Example 3.9.16 concerning a Fuchsian arithmetic group with compact 2-dimensional quotient)
3. an example provided by a quaternion algebra, which illustrates the most general construction of arithmetic Kleinian groups

We start with number fields. This material is really part of the prerequisites; it is included for the benefit of readers whose algebraic number theory may be a bit rusty, but mainly to emphasize the differences between algebraic number fields and quaternion algebras. Even these elementary results are surprisingly nontrivial. I believe most of the material is due to Dedekind; my presentation will be fairly close to that of Samuel [75].

D4.1 Algebraic number theory: a crash course

An *algebraic number field* is a field K containing $\mathbb{Q}$ such that K as a vector space over $\mathbb{Q}$ has finite dimension d, known as the *degree* of K over $\mathbb{Q}$ (see Exercise D4.1.2). We denote this degree by $[K : \mathbb{Q}]$. When $\mathbb{Q} \subset K' \subset K$, the algebraic number field K can also be viewed as a vector space over K'; its dimension as a vector space over K' is denoted by $[K : K']$.

In the setting of algebraic number theory, it is often (even usually) the case that there is more than one possible field of scalars over which K will be a vector space. It almost always matters which field is being used.

Exercise D4.1.1 Show that $[K : \mathbb{Q}] = [K : K'] [K' : \mathbb{Q}]$. $\diamondsuit$

Exercise D4.1.2 Let $\mathbb{Q}[X]$ be the ring of polynomials with coefficients in $\mathbb{Q}$, and let $p \in \mathbb{Q}[X]$ be an irreducible polynomial of degree d generating an ideal (p). Show that (p) is a maximal ideal in the ring $\mathbb{Q}[X]$, and that $\mathbb{Q}[X]/(p)$ is an algebraic number field of degree d over $\mathbb{Q}$. $\diamondsuit$

We will see in a moment that all algebraic number fields are of this form.

Embeddings of number fields

Theorem D4.1.3 *Let K be an algebraic number field of degree d. There are then at least d distinct embeddings $\sigma_i : K \to \mathbb{C}$.*

PROOF First assume $K = \mathbb{Q}[X]/(p)$ for some irreducible polynomial p of degree d. By the fundamental theorem of algebra, p admits exactly d distinct complex roots $z_1, \ldots, z_d$. We can then define σ_i by $\sigma_i(X) = z_i$. These define embeddings $K \to \mathbb{C}$; they are distinct, and they are the only such embeddings, since any $\sigma : K \to \mathbb{C}$ must map X to a root of p.

For the general case, let K be an algebraic number field of degree d over $\mathbb{Q}$, and let $K' \subset K$ be a subfield of maximal degree d' that admits at least d' distinct embeddings $\sigma_1, \ldots, \sigma_{d'} : K' \to \mathbb{C}$. We will show that the hypothesis $d' < d$ leads to a contradiction.

If $d' < d$, then there exists $\beta \in (K - K')$, which must satisfy a minimal polynomial p_β over K', of some degree $d'' > 1$. We will extend each σ_i to $\sigma_{i,j} : K'[X]/(p_\beta) \to \mathbb{C}$ for $1 \leq j \leq d''$ as follows. The coefficients of p_β are elements of K', not complex numbers. Applying σ_i to these coefficients gives us a complex polynomial $p_{\beta,i}$ with d'' distinct complex roots $z_{i,1}, \ldots, z_{i,d''}$. We can extend σ_i by setting $\sigma_{i,j}(X) := z_{i,j}$. As above, the $\sigma_{i,j}$ are distinct: if $\sigma_{i_1,j_1} = \sigma_{i_2,j_2}$, then σ_{i_1,j_1} and σ_{i_2,j_2} coincide on K', so $i_1 = i_2$, and then $j_i = j_2$ since the roots of $p_{\beta,i}$ are distinct. Thus $K'[X]/(p_\beta) \subset K$ is a subfield of degree $d'd'' > d'$ that admits at least $d'd''$ distinct embeddings into $\mathbb{C}$, contradicting the hypothesis that d' is maximal. □

Corollary D4.1.4 *Let K be an algebraic number field of degree d. Then there exists $\alpha \in K$ such that $K = \mathbb{Q}(\alpha)$, i.e., the smallest subfield of K that contains α is all of K. If p is the minimal polynomial of α over $\mathbb{Q}$, there exists a unique isomorphism $\mathbb{Q}[X]/(p) \to K$ taking the class of X to α.*

Such an α is called a *primitive element* of K over $\mathbb{Q}$.

PROOF Let $\sigma_1, \ldots, \sigma_d$ be distinct embeddings $K \to \mathbb{C}$, and let $K_{i,j}$ be the subfield where $\sigma_i = \sigma_j$, for $i \neq j$ in $\{1, \ldots, d\}$. As a vector space $K_{i,j}$ has dimension strictly less than d. No vector space over an infinite field is the union of finitely many subspaces of lower dimension, so there exists $\alpha \in K - \cup_{i \neq j} K_{i,j}$. The complex numbers $\sigma_i(\alpha)$ are distinct, so the minimal polynomial p of α over $\mathbb{Q}$ has at least d distinct roots in $\mathbb{C}$, namely the $\sigma_i(\alpha)$, for $i \in \{1, \ldots, d\}$. Thus $[\mathbb{Q}(\alpha), \mathbb{Q}] \geq d$, but $\mathbb{Q}(\alpha) \subset K$ so $[\mathbb{Q}(\alpha), \mathbb{Q}] \leq d$; we deduce that $\mathbb{Q}(\alpha) = K$. Thus $\deg p = d$ and since p is a minimal polynomial it is irreducible, so $\mathbb{Q}[X]/(p)$ is a field. Since $p(\alpha) = 0$,