Notation and conventions

The letters $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}_p$ will have the usual meaning. By *positive* number we mean a real number > 0. By $[x]$ we denote the *integral part* of the number $x \in \mathbb{R}$, i.e., the largest integer m with $m \leq x$.

If k is a field, we shall denote by $\bar{k}$ an algebraic closure.

For a (commutative) ring R, we shall denote by R^* the group of invertible elements in R.

By the *rank* of an abelian group Γ, written multiplicatively, we shall mean the maximum number of elements $\gamma_1, \ldots, \gamma_r \in \Gamma$ such that no relation exists of the shape $\gamma_1^{a_1} \cdots \gamma_r^{a_r} = 1$ with integer exponents a_i not all zero. For instance, a torsion group has rank 0.

By *algebraic variety* we mean a subset of an affine or projective space, defined by a set of algebraic equations; we do not insist that the variety is irreducible. In saying that a variety $\mathcal{X}$ is defined over a field k, we mean that it may be defined by a set of equations with coefficients in k, and we sometimes write $\mathcal{X}/k$; we usually identify the variety with the set of its points over an algebraic closure of k. Usually we shall consider varieties defined over $\bar{\mathbb{Q}}$ (or occasionally over $\mathbb{C}$ or some finite field).

For an algebraic variety $\mathcal{X}$ defined over k, we denote by $k(X)$ the field of rational functions on $\mathcal{X}$ with coefficients in k. By $\mathcal{X}(k)$ we mean the set of points of $\mathcal{X}$ with coordinates in k. By *algebraic point* we usually mean a point in $\mathcal{X}(\bar{\mathbb{Q}})$.

Usually, capitals X_i will denote variables over a ground field k. If $f \in k[X_1, \ldots, X_n]$ and if σ is an automorphism of k, f^σ will denote the polynomial obtained by applying σ to the coefficients of f.

If $\mathcal{X}$ is a variety defined by equations $f_i = 0$ over a field k, by $\mathcal{X}^\sigma$ we mean the variety defined by the equations $f^\sigma = 0$. It is easy to see (using the Nullstellensatz) that this does not depend on the set of defining equations.

The expression "$f \ll g$", for complex functions f, g of a variable x, will mean as usual that $|f(x)| \leq c|g(x)|$ for an unspecified number c, independent of x but which may depend on other data, thought of as fixed as x varies. (This is occasionally indicated explicitly by writing, e.g., "$f \ll_{S,\varepsilon} g$".)

We have often used the word "algorithm" to mean a procedure which leads to the solution of the relevant problem in finite time. We stress that all the algorithms presented in this book allow us to estimate the running time for actual computation in terms of standard functions.

A few theorems are stated but not proved here; this is indicated with a star.