Errata of the PhD thesis
'Random Walks on Arakelov Class Groups'

Koen de Boer

September 29, 2022

1 Introduction

2 Preliminaries

- Page 55, equation (2.11) should be

$$\rho_K = \lim_{s \to 1} (s-1)\zeta_K(s) = \frac{2^{n_{\mathbb{R}}} \cdot (2\pi)^{n_{\mathbb{C}}} \cdot R_K \cdot h_K}{|\mu_K| \cdot \sqrt{|\Delta_K|}},$$

  that is, with an additional equation sign '='.

3 The Continuous Hidden Subgroup Problem

4 Random Walks on Arakelov Ray Class Groups

5 A Worst-case to Average-case Reduction for Ideal Lattices

6 Ideal Sampling

7 The Power Residue Symbol is in ZPP

- Page 262, Algorithm 9, the 'Ensure:' line should read:
  Ensure: $\left(\frac{\mathfrak{b}}{L/K}\right) \in \mathrm{Gal}(L/K)$, or failure.

8 Appendices