Explicit bounds for a generating set of the class group (under GRH)

Giuseppe Molteni

Università di Milano

Let $\mathcal{C}\ell_{\mathbb{K}}$ be the class group of the number field $\mathbb{K}$ over $\mathbb{Q}$. Let Δ be the absolute value of the absolute discriminant of $\mathbb{K}$, let n denote the degree of $\mathbb{K}$ as extension of $\mathbb{Q}$ and r_2 the number of pairs of complex imbeddings of $\mathbb{K}$. It is known that $\mathcal{C}\ell_{\mathbb{K}}$ is a finite and abelian group. In order to detect its structure it is necessary to know a set of generators. Minkwoski's bound shows that the set of all classes of all prime ideals with norm $\leq \left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}\sqrt{\Delta}$ is such a set. This bound has been improved by Zimmert in its explicit dependence of the degree, but the dependence on the discriminant is still via $\sqrt{\Delta}$. This is a problem for numerical computations since the discriminant grows very quickly with the degree so that the bound becomes essentially unfeasible also for fields with moderate degree. Following a suggestion of Stark, Eric Bach [1] proved that under the Generalized Riemann Hypothesis the bound improves dramatically to $12\log^2\Delta$ for all fields, and to $(4+o(1))\log^2\Delta$ asymptotically.

In the seminar I will show how it is possible to further improve the bound to

$$\min(4.01\log^2\Delta, 4(\log\Delta+\log\log\Delta-4n+2)^2)$$

for all fields, and to $4\log^2\Delta$ whenever $\log\Delta \leq 11^n/e$ (better but more complicated bounds are also possible). The result has been obtained in collaboration with Loïc Grenié [2].

[1] E. Bach, *Explicit bounds for primality testing and related problems*, Math. Comp. **55** (1990), no. 191, 355–380. DOI: 10.2307/2008811.

[2] L. Grenié, and G. Molteni, *Explicit bounds for generators of the class group*, Math. Comp. **87** (2018), no. 313, 2483–2511. DOI: 10.1090/mcom/3281.