On computable elements of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$

Daniel Miller

August 7, 2016

M. Mignotte: An inequality about factors of polynomials. [Do this for general number fields with height functions.] Are heights effectively computable?

Also see `http://math.stackexchange.com/questions/412010`.

And `http://mathoverflow.net/questions/24047/`

1 Factoring polynomials in number fields

Definition 1. *A* pinned number field *is a monic irreducible polynomial $f \in \mathbf{Z}[x]$.*

When we say "let F be a pinned number field," we mean "let f be a monic irreducible polynomial and $F = \mathbf{Q}[x]/(f)$.

For us, a *pinned number field* consists of a number field F together with a chosen isomorphism $\mathbf{Q}[T]/f \xrightarrow{\sim} F$, where $f \in \mathbf{Z}[T]$ is a specified monic irreducible polynomial.

Claim: the height function $H : O_F \to \mathbf{R}_{>0}$ is computable. Indeed,

$$H(x) = \#(O_F/x) \cdot \prod_{v|\infty} \max\{\|x\|_v, 1\}.$$

and both the set $F(\infty)$ of infinite places of F and the normalized "absolute value" $\|x\|_v$ are computable. For any $c \in \mathbf{R}$, we want the set $\{H < c\}$ to be effectively computable.

Better, use Theorem 2 from [Mig74]: if $g = \sum g_i t^i$ is a factor of $f = \sum f_i t^i$ in $\mathbf{C}[t]$, then

$$\max\{|g_i|\} \leqslant \deg(f)! \left(\sum |f_i|^2\right)^{1/2}$$

In other words, there is an effectively computable constant $C(f)$ such that all coefficients in g have absolute value $\leqslant C(f)$.

2 Conclusion

The idea was to show that there is a dense computable subset of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. It turns out the idea was already figured out by Greg Kuperberg. See his answer to `http://mathoverflow.net/questions/6802`.

References

[Mig74] M. Mignotte. An inequality about factors of polynomials. *Math. Comp.*, 28:1153–1157, 1974.