Finding orders with prescribed index
Project Log

Alex J. Best

December 5, 2013

13/10/13

Implementations exist in Magma (refs) Finding power basis for order with specified index in a given order. 15/10/13

István Gaál has done a lot of work in this area, and there exists(ed) an implementation within KANT (run by Pohst). 16/10/13

Should think up naive algorithm first in a general setting (no power basis etc). Take an absolute number field $K|\mathbb{Q}$ and consider $\mathcal{O} \subset \mathcal{O}_K$ letting $I = [\mathcal{O}_K : \mathcal{O}]$ we should find a relation between I and the conductor of $\mathcal{O}$. Recall the conductor $\mathfrak{f}$ of $\mathcal{O}$ is the largest ideal of $\mathcal{O}_K$ contained in $\mathcal{O}$, so $\mathfrak{f} = \{\alpha \in \mathcal{O}_K \mid \alpha\mathcal{O}_K \subseteq \mathcal{O}\}$. Will probably come down to computing some quotient $\mathcal{O}/\mathcal{N}$. 25/10/13

We have that $\mathcal{O}_K/\mathcal{O} \cong (\mathcal{O}_K/\mathfrak{f})/(\mathcal{O}/\mathfrak{f})$ so we can see $[\mathcal{O}_K : \mathcal{O}][\mathcal{O} : \mathfrak{f}] = [\mathcal{O}_K : \mathfrak{f}]$. As we know the index we wish to obtain we know that the norm of the conductor of the order we are looking for is divisible by the index. This gives us some prime ideals that must divide the conductor so we start with these. We then calculate the possible conductors and their corresponding orders (how?). 7/11/13

Given $[F : \mathbb{Q}] = d$ we have $\mathcal{O}_F \subset F$ and $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_F$. Then $\mathbb{O}_F/\mathcal{O} = \mathcal{O}_F/f\mathcal{O}_f$ torsion module. $\text{norm}(f\mathcal{O}_F) = f^2 \in \mathbb{Z}$.

Can work one prime at a time (locally) then path things together for a speedup.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
∋					𝔘	𝔡	≃	⊒	⊒	⊐	⋖	⋗	⋉	⋊	∣	∥	⟍	∼	≋	≅	≍
w	x	y	z	1	2	3	4	5	6	7	8	9	0								
≋	↶	↷	𝐹	⊮	⊭	⊯	⊉	⊈	⊄	⊅	↚	↛	⊬								

Table 1: Table of mathbb symbols and their intended counterparts

Translation of Über das Lösen von Einheitenund Indexformgleichungen in algebraischen Zahlkörpern mit einer Anwendung auf die Bestimmung aller ganzen Punkte einer Mordellschen Kurve - Chapter 2

If $\mathcal{K}$ is an algebraic number field so has for any $I \in \mathbb{N}$ the set $\{\alpha \in \mathfrak{o}_\mathcal{K} \mid (\mathfrak{o}_\mathcal{K} : \mathbb{Z}[\alpha]) = I\}$ for a result of Győry [25] a finite representative system $\mathfrak{I}_\mathcal{K}(I)$ with respect to $\mathbb{Z}$-equivalence, where two integral algebraic numbers $\alpha, \beta \in \mathfrak{o}_\mathcal{K}$ are called $\mathbb{Z}$-equivalent if $\alpha \pm \beta \in \mathfrak{o}_\mathcal{K}$. The calculation of $\mathfrak{I}_\mathcal{K}(I)$ is called the index form equation. These designations stirred therefore, because an integral basis $\omega_1 = 1, \omega_2, \ldots, \omega_n$ of $\mathfrak{o}_\mathcal{K}$ of a form $\mathfrak{I}_\mathcal{K}(t_1, \ldots, t_n) \in \mathbb{Z}[t_2, \ldots, t_n]$ with the property

exists, since for all $\alpha = x_1\omega_1 + \ldots + x_n\omega_n \in \mathfrak{o}_\mathcal{K}$ with $(\mathfrak{o}_\mathcal{K} : \mathbb{Z}[\alpha]) < \infty$ each

$$(\mathfrak{o}_\mathcal{K} : \mathbb{Z}[\alpha]) = \pm I_\mathcal{K}(x_2, \ldots, x_n)$$

applies.

The shape IK called index form of K with respect to 1; ::: ; ! N . We will in this chapter apply our method for equations on the unit to lots of index form equations. We mainly use the classic method by which the finiteness of Győry IK (I) showed that, the calculation of the efective IK (I) on the lots of finitely many units -