Finding orders with prescribed index in number fields
Project specification

Alex J. Best

December 5, 2013

Introduction

This is the project specification for the project currently entitled "Finding orders with prescribed index in number fields" which is being supervised by Lassina Dembélé. We begin by briefly stating the background to the problem.

Central to the field of algebraic number theory is the concept of a number field such as $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-17}, \sqrt[3]{5})$. Number fields contain subrings known as orders which have a number of useful properties and give us information about the field itself. It is often desirable to obtain orders with specific indices in another order (roughly this measures the relative size of the order). So the aim of this project is to find algorithms that, given a number field order, finds other orders in it that have the specified index.

There are algorithms within the computational algebra system Magma that can perform these calculations, however there are a number of areas where these techniques can be improved upon. For instance it is desirable to be able to do such calculations with relative number fields rather than only in absolute number fields, finding orders in this case does not currently seem to be implemented however.

Performing such computations is in general easier when the number field has small discriminant, or is otherwise simple in structure. We expect this to be the case with our methods also, though it is hoped that improved methods should make it feasible to do this sort of computation with number fields of higher degree.

The maximal order of a number field is its ring of integers, a much studied object, and well known algorithms exist for finding this order ([Poh-Zas89], [Coh93]). However there is less literature concerning non-maximal orders, than there is about the ring of integers.

Objectives

We have a few major objectives in mind that the project will consist of:

1. Survey existing methods of finding orders of given index.
2. Identify the shortcomings of current methods and the requirements of new techniques.
3. Adapt existing methods and attempt to design new algorithms to solve the problem.
4. Implement the methods found in a mathematics package (such as Sage or Magma).
5. Compare the methods obtained with existing ones, discuss which are most effective in different situations.

6. Explore the applications of these methods to elliptic curves over the rational numbers (and elsewhere!).

These objectives will follow on from each other in a linear fashion, so I will work on them in order but likely work on a multiple objectives simultaneously where it is natural to do so.

Proposed Timetable

The following is a provisional timetable listing roughly when the objectives above will be worked on, it is very much subject to change. Some areas will naturally be worked on simultaneously and this is reflected below. The timetable is purposefully ambitious, this is to allow plenty of room for adjustments when objectives take longer than listed here.

Dates	Objectives worked on
10/10/13 - 18/10/13	1
18/10/13 - 25/10/13	1, 2
25/10/13 - 14/11/13	1, 2, 3
14/11/13 - 21/11/13	3, 4
21/11/13 - 1/12/13	4, 5
1/12/13 - 8/12/13	5
8/12/13 - 9/1/14	6

Table 1: Timetable for work on the project

Other remarks

There are no legal, social, ethical and professional issues associated with the project.

Computing resources used will likely be the terminals within the Computer science department, my own personal computer and the server Fermat within the Mathematics department. All of which will of course be kept backed up both online and on the systems within the computer science department.

References

[Coh93] Henri Cohen, *A Course in Computational Algebraic Number Theory*. Springer, 1993.

[Poh-Zas89] M. Pohst and H. Zassenhaus, *Algorithmic algebraic number theory*. Cambridge University Press, 1989.