Finding orders with prescribed index in number fields
Progress report

Alex J. Best

December 5, 2013

Introduction

The project is progressing well overall and there have been no serious issues so far. Below is a non-technical account of the work completed so far and some of the problems encountered.

Included at the end is the original specification for quick reference.

Existing methods and their shortcomings

The main body of existing work on this type of problem concerns itself with so called "index form equations". Moreover, much work on these equations does so with a view to finding power integral bases. The aim of this more specific problem is given the ring of integers $\mathbb{Z}_K$ of some number field K to find $\alpha \in \mathbb{Z}_K$ such that $\mathbb{Z}_K = \mathbb{Z}[\alpha]$. This is reflected in the current implementation of the Magma function IndexFormEquation which returns a single generator α of an order of index d, such an order is known as *monogenic*. As Dedekind first showed, there exist non-monogenic orders for number fields of degree ≥ 3, hence being able to solve equations of the above form, does not always allow us to find all orders with a specified index. Due to the focus of these methods being not completely aligned with the goal of this project there is less existing reference material than originally expected. Nevertheless the existing work still uses relevant techniques and ideas and so studying the material available for solving these equations has been useful for furthering the work.

Current ideas

Sage[1] and Magma[2] are two of the most prominent pieces of software for performing computations in number theory. So it is desirable to work with one of these systems to develop algorithms as they have a number of useful features and structures already implemented well. Upon looking into the functionality of both systems I discovered that Sage is lacking some functions necessary for doing the computations I need. Most notably in Sage there does not seem to be existing implementations to find the conductor of an order nor is there any built in way of constructing a localisation of a ring at a prime ideal. As Sage is open source and welcomes contributions it is possible to not only implement these for our usage, but also to have these modifications adopted into the Sage source code. This is something that I would like to do before the project's completion, however for the purpose of easy experimentation I have elected to use Magma for the present. This has slowed progress a little as I am not as experienced with Magma as I am

[1] http://sagemath.org
[2] http://magma.maths.usyd.edu.au

with Sage. It therefore takes longer to find the correct functions and/or syntax to perform a particular action, this is not helped by the style of the Magma online documentation.

Using Magma a basic algorithm has been implemented to enable us to find the generators of all orders with a given index. This algorithm makes use of the conductor of the order and results relating the norm of the conductor to the index of the order itself. This algorithm, while still fairly naïve, works faster than expected on the inputs I have tested it on and provides good evidence that the approach I have taken to the problem is a good one.

Next steps

As I am very much still on schedule the work to be undertaken over the next few weeks is still as planned in the initial specification. The basic algorithm will be improved upon by using more results to optimise the steps taken. For example, using localisations of orders I hope to break the computations down into smaller ones that can be combined to obtain our results more efficiently. When the general algorithm has been developed to a reasonable level I will continue by exploring optimisations that can be made in special cases. We will also look at how the new methods compare to those already existing in areas where there is overlap. Once this is done I will as per the originally proposed timetable look at the applications of these algorithms to elliptic curves.

Conclusion

The project is progressing well, although there is less existing material to draw on than I originally expected, this is not a significant issue. In fact the lack of work done on the full problem should allow us to come up with more interesting material, rather simply learning and adapting existing approaches. As it currently stands I am confident that I should obtain some nice results as part of the project within the time frame.

Appendix: Original specification

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 ([**?**], [**?**]). 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.