MA3A6 WEEK 8 ASSIGNMENT : DUE MONDAY 4PM WEEK 8

BILL HART

1. Find out the algorithm used by Pari to compute rings of integers of number fields. You may like to look at the Pari documentation, the source code for Pari (both available from the Pari website - linked to from the class website) or post a question on the Pari support list.

The function in Pari for computing this is called **nfbasis**. Looking at the help for this function, it reveals that an algorithm called **round 4** is used. The source code for Pari also mentions this algorithm in the comments.

The details of the algorithm are *very* complicated. It turns out that to compute the maximal order, it is essentially enough to compute an order that is p-maximal for all primes p for which p^2 divides the discriminant of the field. A p-maximal order G of $\mathcal{O}_K$ is a subgroup such that $|\mathcal{O}_K/G|$ is not divisible by p.

The algorithm proceeds by enlarging the order at each step to make it p-maximal for each of the primes p. This enlargement step relies on a criterion developed by Dedekind for determining whether an order is p-maximal. As for the algorithm we use in class, this algorithm also tells one how to enlarge the order if it is not p-maximal.

The criterion of Dedekind works by factoring the minimum polynomial of the generator of K over the field $\mathbb{Z}/p\mathbb{Z}$. One then constructs a certain auxilliary polynomial from the factors and this then gets "lifted" back to a polynomial in $\mathbb{Z}[x]$. There is then a technical condition to check, involving this lifted polynomial.

The round 4 algorithm was originally phrased as a polynomial factorisation algorithm. Essentially one works over $\mathbb{Z}_p$ and ends up constructing an integral basis for the number field as though it were defined by a polynomial with coefficients in $\mathbb{Z}_p$. One computes a maximal order in this setting, and this makes use of the Dedekind criterion as a first step. Very roughly speaking, the field polynomial of an element of the maximal order has the Dedekind test applied to it. This tell one whether the order needs enlarging and if not, how to enlarge it. There are some complications with this method, so other branches of the algorithm deal with such complications, but the details are technical and I won't try to describe them.

2. Write a *short* Pari program to compute rings of integers of the fields generated by one of the roots of each of the polynomials $f(x) = x^3 - 3x + i$ for all $1 \leq i \leq 100$.

I don't know what the minimum is, and I look forward to seeing what you have come up with, once Michael has finished marking, but my best effort was 47 characters, using the built-in function in Pari for computing an integral basis:

```
vector(100,i,nfinit(factor(x^3-3*x+i)[1,1]).zk)
```

3. Determine which algebraic numbers of the form $\alpha = \frac{1}{3}(\lambda_1 + \lambda_2\omega + \lambda_3\omega^2)$ can be algebraic integers for $\lambda_i \in \mathbb{Z}$, $0 \leq \lambda_i \leq 2$ and $\omega^3 = 7$.

As per the example in class, computing the trace of α simply tells us that λ_1 has to be a rational integer, which tells us nothing.

Thus we compute the norm of α. The minimum polynomial of the generator of the field is $x^3 - 7$ and the other roots are $\zeta\omega$ and $\zeta^2\omega$ where ζ is primitive cube root of unity.

The norm of α is therefore

$$\mathcal{N}(\alpha) = \frac{1}{27}(\lambda_1 + \lambda_2\omega + \lambda_3\omega^2)(\lambda_1 + \lambda_2\zeta\omega + \lambda_3\zeta^2\omega^2)(\lambda_1 + \lambda_2\zeta^2\omega + \lambda_3\zeta\omega^2)$$

Expanding this out, we find that the norm is $\frac{1}{27}(\lambda_1^3 - 21\lambda_1\lambda_2\lambda_3 + 7\lambda_2^3 + 49\lambda_3^3)$.

Thus we must check for values of $\lambda_i \in 0 \ldots 2$ such that $\lambda_1^3 - 21\lambda_1\lambda_2\lambda_3 + 7\lambda_2^3 + 49\lambda_3^3 \equiv 0 \pmod{27}$.

If $\lambda_1 = 0$ we must have $7\lambda_2^3 + 49\lambda_3^3 \equiv 0 \pmod{27}$. The cubes of 0, 1 and 2 modulo 27 are $0, 1, 8$. Thus 7 times such a cube must be $0, 1, 2$ and 49 times such a cube is $0, 7, 14$. It is clear that the only solution is $\lambda_2 = \lambda_3 = 0$ if $\lambda_1 = 0$.

If $\lambda_1 = 1$ we must have $1 - 21\lambda_2\lambda_3 + 7\lambda_2^3 + 49\lambda_3^3 \equiv 0 \pmod{27}$. Considering this first modulo 3 we see that the only possibilities are $(\lambda_2, \lambda_3) = (0, 2), (2, 0), (1, 1)$. Substituting these in turn reveals no solutions mod 27.

If $\lambda_1 = 2$ we must have $8 - 15\lambda_2\lambda_3 + 7\lambda_2^3 + 49\lambda_3^3 \equiv 0 \pmod{27}$. Again modulo 3 the only possibilities are $(\lambda_2, \lambda_3) = (0, 1), (1, 0), (2, 2)$. Again, none of these yield solutions modulo 27.

Therefore there are no algebraic integers of the required form, apart from the trivial solution 0.

4. The ring of integers of $\mathbb{Q}(\zeta_5)$ for ζ_5 a primitive 5-th root of unity, is $\mathbb{Z}[\zeta_5]$. Compute the discriminant of $\mathbb{Q}(\zeta_5)$. Check your answer with Pari.

The field has degree 4 and $\{1, \zeta, \zeta^2, \zeta^3\}$ is a $\mathbb{Z}$-basis for the ring of integers. We know that this has discriminant given by

$\Delta[1, \zeta, \zeta^2, \zeta^3] = (-1)^{\frac{4\times(4-1)}{2}}\mathcal{N}(f'(\zeta))$, where $f'(x) = 4x^3 + 3x^2 + 2x + 1$.

The other roots of the minimum polynomial of ζ are $\zeta^2, \zeta^3, \zeta^4$. The value we are after is therefore $(4\zeta^3 + 3\zeta^3 + 2\zeta + 1)(3\zeta^4 + 2\zeta^2 + 4\zeta + 1)(4\zeta^4 + 2\zeta^3 + 3\zeta + 1)(2\zeta^4 + 3\zeta^3 + 4\zeta^2 + 1)$. Expanding this out by multiplying one factor at a time, we get $1975(\zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1) + 125 = 125$.

Checking with Pari

```
f=(x^5-1)/(x-1)
K=nfinit(f)
K.disc
```

we find that this is the correct discriminant.

E-mail address: hart_wb@yahoo.com