MA3A6 WEEK 10 ASSIGNMENT : DUE MONDAY 4PM WEEK 10

BILL HART

1. Show that in a quadratic number field K a rational prime p either:

(i) Splits completely into a product of distinct prime ideals $(p) = \mathcal{P}_1\mathcal{P}_2$.

(ii) Ramifies, $(p) = \mathcal{P}_1^2$.

(iii) Remains inert, i.e. (p) is a prime ideal in $\mathcal{O}_K$.

Consider a rational prime p. When we speak of factoring p in $\mathcal{O}_K$ we are really talking about factoring the ideal $(p) = p\mathcal{O}_K$ in $\mathcal{O}_K$. It's norm in the number field K is going to be p^n where n is the degree of the field, which is 2 in this case, since it is a quadratic field.

When we factor $p\mathcal{O}_K$ in the ring of integers $\mathcal{O}_K$ of K the product of the norms of the prime ideal factors must be equal to the norm of $p\mathcal{O}_K$ which is p^2 in our case.

For ideals whose norm is not 1, i.e. ideals that are not the whole of $\mathcal{O}_K$, their norms must divide p^2. The only possibilities are that we have two prime ideals of norm p or one prime ideal of norm p^2.

If we have two prime ideals of norm p, if the ideals are distinct, then we are in case (i) and if they are the same, we are in case (ii).

If there is only a single prime ideal, it must be $p\mathcal{O}_K$, i.e. p "remains prime" in $\mathcal{O}_K$. We know the norm is then $\mathcal{N}((p)) = |\mathcal{N}(p)| = p^2$. This is case (iii).

This is one of many ways to prove this result. For a relevant result along the lines of my other suggestion in the question sheet, see J. S. Milne's notes on Algebraic Number Theory online (Thm 3.41 in version 3.0 of his notes).

2. Let $S = \{2, 3, 5\}$. Find a number field K such that one of the primes in S ramifies in K, one of them splits completely and the other is inert in K.

I used Pari to initially find such a number field. I discovered that the conditions were met for the number field $K = \mathbb{Q}(\sqrt{-2})$. Recall that the discriminant here is -8 since it has to be 0 or 1 mod 4. The only primes dividing the discriminant are 2, thus 2 is ramified in K.

We can factor 3 and 5 in K since the ring of integers of K is $\mathcal{O}_K = \mathbb{Z}[\sqrt{-2}]$ and $\sqrt{-2}$ is an algebraic integer with minimum polynomial $x^2 + 2$.

We factor the minimum polynomial modulo 3 and 5. Modulo 3 we obtain $x^2 + 2 \equiv x^2 - 1 \equiv (x + 1)(x - 1) \pmod 3$. Thus (3) factors into two distinct prime ideals in $\mathcal{O}_K$, as $(x - 1)$ is not congruent to $(x + 1)$ modulo 3.

Modulo 5 we see that $x^2 + 2$ is irreducible (any factor would be linear, giving a root of $x^2 + 2$ in $\mathbb{Z}/5\mathbb{Z}$, but substituting each of the values modulo 5 into $x^2 + 2$ we see it has no roots in this field). Thus (5) remains prime in $\mathcal{O}_K$, i.e. it is inert.

3. Let $K = \mathbb{Q}(\alpha)$ be the number field with α a root of $x^5 + 7x^4 + 3x^2 - x + 1$.

(The function poldisc(f) in Pari will give you the discriminant of a general polynomial f, i.e. it will basically give you the discriminant of $\mathbb{Z}[\alpha]$ for α a root of f.)

Using Pari, compute discriminants of $\mathcal{O}_K$ and $\mathbb{Z}[\alpha]$ and by hand (without Pari), use this information, to factorise the rational prime 5 in $\mathcal{O}_K$.

The problem we have is that we do not know the ring of integers of K. But we do know that $R = \mathbb{Z}[\alpha]$ is an order contained in the ring of integers and that α is an algebraic integer.

We compute the discriminant of K, which is the discriminant of a $\mathbb{Z}$-basis for the ring of integers of K. Pari tells us it is 2945785.

We also compute the discriminant of $\mathbb{Z}[\alpha]$ using poldisc. Pari tells us that it is the same. This tells us that $\mathbb{Z}[\alpha]$ actually is the ring of integers of K (to be sure this is cheating, but it is too hard to compute the ring of integers by hand).

We now use our theorem about factoring rational primes in rings of integers to factor 5. This means we must factor $x^5 + 7x^4 + 3x^2 - x + 1$ modulo 5. Actually there is a simpler way of doing this than what I previously showed the class. I type $\text{factor}(\text{Mod}(1,5) * x^5 + \text{Mod}(7,5) * x^4 + \text{Mod}(3,5) * x^2 - \text{Mod}(1,5) * x + \text{Mod}(1,5))$.

It tells me the factors are $(x + 2)$, $(x + 3)^2$ and $(x^2 + 4x + 2)$.

To get the prime ideal factors of (5), I simply plug α into each of these and I get that the prime factorisation is:

$(5) = (5, \alpha + 2)(5, \alpha + 3)^2(5, \alpha^2 + 4\alpha + 2)$.

4. Find out the Pari function for factoring rational primes into prime ideals in a number field. Use this function to write a short program to factor the first 10 rational primes into prime ideals in $\mathbb{Q}(\alpha)$ for α a root of $x^3 - 3x^2 + 3x + 1$. Examine the output Pari gives you carefully (and refer to the technical documentation describing the output) and use this output to determine which of these 10 rational primes ramify, which are inert and which split completely in K.

I type:

$k = \text{nfinit}(x^3 - 3 * x^2 + 3 * x + 1)$

$\text{for}(i = 1, 10, \text{print}(\text{idealprimedec}(k, \text{prime}(i))))$

In each case, the rational prime p factors as a number of prime factors represented in the form:

$[p, [a, b, c]\ , e, f, [d, e, f]\ ]$

This is an ideal dividing p with ramification index e and with residue class degree f.

If the prime is ramified, the ramification index e would be larger than 1 for one of its prime ideal factors. If the prime p splits completely then for all its factors both e and f will be 1. If the prime is inert, there will be only one prime ideal factor and e will be 1.

We see from the output that 2 and 3 are ramified, 7, 13 and 19 are inert and none of the primes split completely.

E-mail address: hart_wb@yahoo.com