MA3A6 WEEK 6 ASSIGNMENT : DUE MONDAY 4PM WEEK 6

BILL HART

1. Prove that if we take the monic polynomial of least degree of which an algebraic integer α is a root, that it has rational integer coefficients.

Since α is an algebraic integer, it is a root of a monic polynomial $g(x)$ with rational integer coefficients. The minimum polynomial $f(x)$ of α must be a factor of $g(x)$ over $\mathbb{Q}[x]$.

To prove the required fact, we use Gauss' lemma. It states:

Thm: Let $g(x) \in \mathbb{Z}[x]$ and suppose that $g(x) = h_1(x)h_2(x)$ with $g(x), h(x) \in \mathbb{Q}[x]$. Then there exists $\lambda \in \mathbb{Q}$, $\lambda \neq 0$ such that $\lambda h_1(x), \lambda^{-1}h_(x) \in \mathbb{Z}[x]$.

In other words, if we can factor $g(x)$ over $\mathbb{Q}[x]$, then we can factor it over $\mathbb{Z}[x]$.

But since $g(x)$ is monic, then its factors over $\mathbb{Z}[x]$ must also be monic (or they can be made so upon multiplication by -1). Then $f(x)$ must divide one of these factors. We keep doing this, until we get to a monic polynomial of the same degree as $f(x)$, of which $f(x)$ must be a factor. But such a polynomial must be $f(x)$ itself, as $f(x)$ is monic. In other words, $f(x) \in \mathbb{Z}[x]$ as was required.

2. How many units does $\mathbb{Q}(\sqrt{d})$ have if d is a negative fundamental disciminant?

Let $d = -m$ with m positive. If $d \equiv 1 \pmod 4$ then the ring of integers of $\mathbb{Q}(\sqrt{d})$ is $\mathbb{Z}\left[\frac{1+\sqrt{-m}}{2}\right]$. An element of this ring has the form $\frac{a+b\sqrt{-m}}{2}$ with a and b of the same parity. The norm of such an element is $(a^2 + mb^2)/4$. The only way this can have norm ± 1 is if $a^2 + mb^2 = 4$, since m is positive.

Regardless of the value of m, $(a, b) = (\pm 2, 0)$ are always solutions, corresponding to the units ± 1.

But since $d \equiv 1 \pmod 4$, $m \geq 3$. If $m = 3$ there is the special solution $(a, b) = (\pm 1, \pm 1)$. Along with ± 1 these four solutions give the 6-th roots of unity. Thus for discriminant $d = -3$ there are six units. In all other cases there are 2 units (just ± 1).

In the case where $m \equiv 0 \pmod 4$ the ring of integers has the form $\mathbb{Z}[\sqrt{-n}]$ where $m = 4n$. Elements of this ring have the form $a + b\sqrt{-n}$. The norm of such an element is $a^2 + nb^2$. For this to be ± 1 we need either $(a, b) = (\pm 1, 0)$ corresponding to the units ± 1 again, or we need $n = 1$ and $(a, b) = (0, \pm 1)$. So in the case of discriminant $d = -4$ we have four units $1, -1, i, -i$, otherwise there are just two.

So with two exceptions, $\mathbb{Q}(i) = \mathbb{Q}(\sqrt{-4})$ and $\mathbb{Q}(\sqrt{-3})$, imaginary quadratic number fields have just two roots of unity ± 1.

3. Factorise $14 + 12i$ into irreducibles in $\mathbb{Z}[i]$.

Clearly we can break it down into $2(7 + 6i)$. We can take norms of the two factors (the norms are $4 = 2 \times 2$ and $(7 + 6i)(7 - 6i) = 85 = 17 \times 5$) and look for elements of norm 2, 5 and 17 in $\mathbb{Z}[i]$.

We quickly find $14 + 12i = (1 + i)(1 - i)(2 + i)(4 + i)$. We check the norms of all the factors are 2, 2, 5 and 17 respectively, which are all rational primes. Thus we have broken $14 + 2i$ down into irreducibles.

4. Prove that the ring of integers of $K = \mathbb{Q}(\sqrt{-2})$ has unique factorisation.

To prove this, we'll show that the ring of integers $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain.

To do this we need a Euclidean function, and $|\mathcal{N}(-)|$ will do.

The proof of this is identical to the proof we completed in class for $\mathbb{Z}[i]$.

By what we proved in class, it is enough to show that for any $\epsilon = a + b\sqrt{-2} \in \mathbb{Q}(\sqrt{-2})$, with $a, b \in \mathbb{Q}$ there is a $\kappa = r + s\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$, with $r, s \in \mathbb{Z}$, with $|\mathcal{N}(\epsilon - \kappa)| < 1$, i.e. $|(r-a)^2 + 2(s-b)^2| < 1$.

But to prove this we can take r, s to be the nearest integers to a, b respectively. Then $|(r-a)^2 + 2(s-b)^2| \leq |(1/2)^2 + 2(1/2)^2| = 3/4 < 1$, and we are done.

E-mail address: hart_wb@yahoo.com