MA3A6 "WEEK 11" ASSIGNMENT : NOT ASSESSED

BILL HART

1. Find a group of units of finite index in the full unit group of $\mathbb{Q}(\sqrt{2})$. Write the units of your group in terms of a set of generators for the group and show that all the units represented in this way are actually distinct. Note that you can use Dirichlet's unit theorem for the former, but not the latter.

Recall that Dirichlet's Unit Theorem states that the group of units is finitely generated of rank $r + s - 1$ where r is the number of real embeddings and s is half the number of complex embeddings.

If we find a group of units of this rank, we must have a group of finite index in the full group. Note that even if we compute the torsion part of the full group of units (the roots of unity) we still may not have the full unit group. But the question doesn't require this (that would be a set of fundamental units which is much harder to compute).

In the case in question there are two real embeddings and zero complex embeddings, so the rank is $r + s - 1 = 2 + 0 - 1 = 1$.

We easily see by taking norms that $\epsilon = 1 + \sqrt{2}$ is a unit in the ring of integers. Thus all powers of ϵ are also units in the ring of integers of this field.

If we can show that all integer powers (positive and negative) ϵ^n are distinct, then we will have a subgroup $< \epsilon >$ of the full group of units, which is of rank 1 and hence of finite index in the full group of units.

But suppose that $\epsilon^m = \epsilon^n$ for some $m, n \in \mathbb{Z}$. Then $\epsilon^{m-n} = 1$, i.e. ϵ would be a root of unity. But the complex norm of ϵ is $1 + \sqrt{2}$ which is not 1, thus this unit does not lie on the unit circle in the complex plane and so cannot be a root of unity.

Another way of proceeding with this question is to use induction. One considers the non-negative powers of $\epsilon = 1 + \sqrt{2}$ and shows they are all distinct. The induction step starts with $\epsilon^n = a + b\sqrt{2}$ for some $a, b \in \mathbb{N}$ and proceeds to show that $\epsilon^{n+1} = c + d\sqrt{2}$ for some c, d bigger than a, b respectively.

All students should work through such an induction argument, filling in the many missing details and convincing themselves that it works.

2. Use Minkowski's bound to compute the class number (order of the class group) of $\mathbb{Q}(\sqrt{10})$. Recall that Minkowski's result only gives you a bound on the class number, you have to actually find all ideals with norm below that bound to actually determine the class number.

This is discussed in detail in section 10.3 of the textbook. The discriminant $d = 40$, the degree of the field is $n = 2$ with two real embeddings $r = 2$ and zero complex embeddings $s = 0$ (the book uses s, t instead of r, s).

The Minkowski theorem states that every class of ideals contains an ideal of norm less than or equal to $\left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|d|}$. In our case this bound is $0.5\sqrt{40}$ which is just above 3. So we must factorise the primes less than or equal to 3.

We find 3 factors as $\mathfrak{g}_1\mathfrak{g}_2 = (3, 1 + \sqrt{10})(3, 1 - \sqrt{10})$ and 2 factors as the square of a prime ideal $\mathfrak{p}$. We first prove that $\mathfrak{p}$ is not principal, thus the class number is at least 2, since not all the ideals are principal ideals.

But the question remains as to whether $\mathfrak{p}$, $\mathfrak{g}_1$ and $\mathfrak{g}_2$ are in separate ideal classes. To determine this, we take the product of the ideals $\mathfrak{p}\mathfrak{g}_1 = (-2 + \sqrt{10})$ which is principal. Thus the class of $\mathfrak{g}_1$ must be the inverse of the class of $\mathfrak{p}$. But as $\mathfrak{p}^2$ is principal, the classes of $\mathfrak{p}$ and the inverse must be the same. Thus $\mathfrak{g}_1$ is in the same class as $\mathfrak{p}$.

A similar argument shows that $\mathfrak{g}_2$ is in the same class.

Thus there is only one non-principal class and the class number must be exactly 2.

See the textbook for some of the missing details.

E-mail address: hart_wb@yahoo.com