PMath 441/741 – Homework 10 Solutions

1. Let K be a number field of degree 3 over $\mathbb{Q}$, with ring of integers $\mathcal{O}_K$. If the unit group $\mathcal{O}_K^*$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}^2$, how many real embeddings does K have?

Solution: Well, we know that $r + 2s = 3$ (because $r + 2s$ is the degree), and $r + s - 1 = 2$ (because the unit group has rank two). The second equation gives $r + s = 3$, so obviously $s = 0$ and $r = 3$. So K has 3 real embeddings. ♣

2. Let $K = \mathbb{Q}(\sqrt{-10})$, and let $L \neq K$ be a number field containing K. Prove that $\mathcal{O}_K^* \neq \mathcal{O}_L^*$.

Solution: For K, we have $r_K + s_K - 1 = 0 + 1 - 1 = 0$, so the unit group has rank zero. (In fact, it's not too hard to see that it's ± 1.) If L is a number field containing K, then we must have $s_L \geq 1$ (because the complex embedding of K will extend to a complex embedding of L).

But the degree of L is strictly larger than the degree of K, so $r_L + 2s_L > 2$. This means either $r_L > 0$ or $s_L > 1$, and in either case, we get $r_L + s_L > 1$. So the unit group $\mathcal{O}_L^*$ of L has infinite order, and is therefore different from $\mathcal{O}_K^*$. ♣

3. Let L and K be number fields with rings of integers $\mathcal{O}_K$ and $\mathcal{O}_L$, respectively. Is it possible to have $L \neq K$ but $\mathcal{O}_K^* = \mathcal{O}_L^*$? If no, then prove it. If yes, then give a specific counterexample.

Solution: Sure, this is easy. Pick $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{-13})$. Both have finite unit groups (because in both cases, $r + s - 1 = 0$), so we just need to compute the roots of unity in each field. For $\mathbb{Q}$, that's obviously just ± 1. For $\mathbb{Q}(\sqrt{-13})$, that's slightly trickier. If you've seen the argument before, then you can stop here. But just in case you haven't, I've reproduced it below.

Say that a primitive nth root of unity ζ_n is contained in $\mathbb{Q}(\sqrt{-13})$. We want to show that $n = 1$ or $n = 2$.

Well, $\mathbb{Q}(\sqrt{-13})$ has degree two over $\mathbb{Q}$, so that means ζ_n also has degree two (or one, but that's not an interesting possibility). But the degree of ζ_n over $\mathbb{Q}$ is $\phi(n)$, where ϕ is the Euler totient function. And we know that if $n = p_1^{a_1} \dots p_r^{a_r}$ is a prime factorization of n, then

$$\phi(n) = (p_1 - 1)p_1^{a_1 - 1} \dots (p_r - 1)p_r^{a_r - 1}$$

In particular, if p is a prime factor of n, then $p-1$ divides $\phi(n)$.

In our case, $\phi(n) = 2$. So there can't be any prime factors of n larger than 3. A slightly closer analysis reveals that 9 can't be a factor of n either, nor can 8 be a factor. This – plus a couple of quick checks – narrows down the possibilities for n to a finite list:

$$n \in \{1, 2, 3, 4, 6\}$$

For $n = 1$ and $n = 2$, we get $\zeta_n = \pm 1$, which is fine.

For $n = 3$ and $n = 6$, ζ_n generates the field $\mathbb{Q}(\sqrt{-3})$. Which isn't L.

For $n = 4$, we get $\zeta_n = \pm i$, which obviously generates the field $\mathbb{Q}(i)$. Which is again, not L.

So L doesn't actually contain any roots of unity other than ± 1. So $\mathcal{O}_L = \mathcal{O}_K$. ♣

4. Find all the roots of unity contained in $K = \mathbb{Q}(\sqrt[4]{-7})$.

Solution: The roots of unity in K are just ± 1.

Any root of unity contained in $\mathbb{Q}(\sqrt[4]{-7})$ must generate a field of degree 1, 2, or 4 over $\mathbb{Q}$. There's a short list of these: they are ζ_n for $n \in \{1, 2, 3, 4, 5, 6, 8, 10, 12\}$, giving the following list of fields:

$$\mathbb{Q},\ \mathbb{Q}(\sqrt{-3}),\ \mathbb{Q}(i),\ \mathbb{Q}(\zeta_5),\ \mathbb{Q}(\zeta_8),\ \mathbb{Q}(\zeta_{12})$$

Obviously K contains $\mathbb{Q}$, so it contains the roots of unity ± 1.

All of these fields are galois over $\mathbb{Q}$, while K is not. So K cannot *equal* any of them, and so in particular K cannot contain ζ_n for $n \in \{5, 8, 10, 12\}$.

It's not too hard to see that K contains the quadratic field $\mathbb{Q}(\sqrt{-7})$. If K were to contain a different quadratic field $\mathbb{Q}(\sqrt{d})$ as well, then it would also have to contain the quartic field $L = \mathbb{Q}(\sqrt{-7}, \sqrt{d})$.

But L has degree four over $\mathbb{Q}$, so if $L \subset K$, we get $L = K$. Since L is galois, this is impossible.

So K doesn't contain ζ_3, ζ_4, or ζ_6 either. That leaves just ± 1. ♣

5. Find generators for the group of units of the ring $\mathbb{Z}[\sqrt{26}]$. Be sure to give a careful proof that your generators do indeed generate.

Solution: First, the Dirichlet Unit Theorem tells us that since $\mathbb{Q}(\sqrt{26})$ has two real embeddings and no complex ones, the unit group of $\mathbb{Z}[\sqrt{26}]$ is isomorphic to $\{\pm 1\} \times \mathbb{Z}$. (The real embedding means that the roots of unity

are just ± 1.) All we need to do is find a unit u of infinite order that is not a power of any other unit, and we'll know that $\mathbb{Z}[\sqrt{26}]^* \cong \{\pm 1\} \times \langle u \rangle$.

The next thing to notice is that $5 + \sqrt{26}$ is a unit, because its norm is -1. It's easy to see that it has infinite order (because it's real and isn't ± 1). Let's check to see if this unit is a power of any other units.

The unit $5 + \sqrt{26}$ corresponds (roughly) to the vector $(10.1, -.1)$. If u is a nontrivial power of another vector $(x, y) \in \mathbb{R}^2$, then $0 < x < 4$ (because $4^2 > 5 + \sqrt{26}$) and $-1 < y < 1$. (We don't have to worry about the negative values of x, because if x is negative, any odd power of (x, y) will have negative first coordinate, and any even power will have positive second coordinate.) In particular, the length of (x, y) is at most $\sqrt{4^2 + (-1)^2} = \sqrt{17}$, which is less than 4.2.

An integral basis of $\mathbb{Z}[\sqrt{26}]$ is $\{1, \sqrt{26}\}$, corresponding to the vectors $(1, 1)$ and $(\sqrt{26}, -\sqrt{26})$. Since these two vectors are orthogonal to each other, the length of the vector $a(1, 1) + b(\sqrt{26}, -\sqrt{26})$ is just $\sqrt{a^2\sqrt{2} + b^2(2\sqrt{13})}$. Since $2\sqrt{13} > \sqrt{17}$, this length is less than $\sqrt{17}$ only when $b = 0$, so the only elements of $\mathbb{Z}[\sqrt{26}]$ in this box are elements of $\mathbb{Z}$. Since those can't be units of infinite order, we know that $5 + \sqrt{26}$ is not a nontrivial power of another element of $\mathbb{Z}[\sqrt{26}]$, so $\mathbb{Z}[\sqrt{26}]^* \cong \{\pm 1\} \times \langle 5 + \sqrt{26} \rangle$. ♣

6. Find an extension of number fields L/K, with rings of integers $\mathcal{O}_K$ and $\mathcal{O}_L$, respectively, such that $\mathcal{O}_L^*$ contains a unit of infinite order that is not contained in $\mathcal{O}_K^*$, but that the rank of $\mathcal{O}_L^*$ is the same as the rank of $\mathcal{O}_K^*$.

Solution: We need K and L to have the same value of $r + s - 1$. But they can't be the same field. Hmm.

We also need the degree of $K/\mathbb{Q}$ to divide evenly into the degree of $L/\mathbb{Q}$, because $K \subset L$. How can we do that and still have the same value of $r+s-1$?

The degree of K over $\mathbb{Q}$ is $r_K + 2s_K$. The degree of L is $r_L + 2s_L$. But we also have

$$r_K + s_K = r_L + s_L$$

So we actually know that $r_K + 2s_K$ is a divisor of $r_K + s_K + s_L$. The quotient is:

$$\frac{r_K + s_K + s_L}{r_K + 2s_K} = \frac{r_K + s_K}{r_K + 2s_K} + \frac{s_L}{r_K + 2s_K}$$

where that first fraction is obviously at most 1, and the second fraction is less obviously at most one, because $s_L = r_K + s_K - r_L \leq r_K + s_K$.

But the whole thing has to be at least two! So each fraction individually must be exactly one, meaning $s_K = 0$ and $r_L = 0$. In other words, K is totally real (has only real embeddings), and L is totally imaginary (has only complex embeddings). And L is a quadratic extension of K.

The easiest case to try is the case $r + s - 1 = 0$. Sadly, this won't work, because then the unit groups have rank zero, so there aren't any units of infinite order in K or L.

So we try $r + s - 1 = 1$. This is where we hit paydirt.

In this case, K is a real quadratic extension of $\mathbb{Q}$ ($r = 2$, $s = 0$), and L is a quartic extension ($r = 0$, $s = 2$). The unit groups $\mathcal{O}_K^*$ and $\mathcal{O}_L^*$ both have rank one. All we have to do is force $\mathcal{O}_L^*$ to have an extra unit of infinite order.

(Incidentally, K and L are called CM-fields. The "CM" stands for "complex multiplication" – this term is used for old-timey reasons that don't really make sense any more. But I'm sure they did at the time.)

So here's an idea. Let's pick a real quadratic extension K of $\mathbb{Q}$, and a unit u in there that's negative. Then we can define L to be $K(\sqrt{u})$. This L has to be totally imaginary, because u has no real square roots. So the unit groups have to be the same rank, and they have to be different because $\sqrt{u}$ is a unit of $\mathcal{O}_L$ that's blatantly not in $\mathcal{O}_K^*$.

Thus, we could take $K = \sqrt{2}$, $u = -1 - \sqrt{2}$, and $L = K(\sqrt{-u})$. There are lots of other examples, but this is the simplest one I could think of. ♣