PMath 441/641 – Homework 2 Solutions

1. Let $p \in \mathbb{Z}$ be a prime number with $p \equiv 3 \pmod 4$. Prove that $\mathbb{Z}[i]/(p)$ is a field.

Solution: We have $\mathbb{Z}[i]/(p) \cong \mathbb{Z}[x]/(x^2+1, p) \cong (\mathbb{Z}/p\mathbb{Z})[x]/(x^2+1)$, which is a field if and only if x^2+1 is irreducible modulo p. A quadratic polynomial is irreducible if and only if its roots do not lie in its coefficient field. The roots of x^2+1 are the two elements of order 4 in the multiplicative group of the field $\mathbb{F}_{p^2}$ with p^2 elements. The multiplicative group of $\mathbb{Z}/p\mathbb{Z}$ is cyclic of order $p-1$, so it contains elements of order exactly 4 if and only if $p-1$ is a multiple of 4, which is precisely the same as saying $p \equiv 1 \pmod 4$. Thus, if $p \equiv 3 \pmod 4$, then $\mathbb{Z}/p\mathbb{Z}$ does not contain any elements of order 4, so x^2+1 is irreducible modulo p, so $\mathbb{Z}[i]/(p)$ is a field. ♣

2. Let $K = \mathbb{Q}(\sqrt{33})$. Compute the trace and norm of the following elements of K:

- $\sqrt{33}$
- 1
- $6 + \sqrt{33}$

Solution: The calculations are straightforward from the definitions. The answers are given in the following table.

α	$N(\alpha)$	$\mathrm{Tr}(\alpha)$
$\sqrt{33}$	-33	0
1	1	2
$6+\sqrt{33}$	3	12

3. Let α be a root of the polynomial $f(x) = 9x^3 + 2x + 7$. Find an integer n such that $n\alpha$ is an algebraic integer.

Solution: The trick to this is to figure out the minimal polynomial for $n\alpha$. It's the polynomial you get when you substitute y/n for x in $f(x)$:

$$9\left(\frac{y}{n}\right)^3 + 2\left(\frac{y}{n}\right) + 7 = \frac{9}{n^3}y^3 + \frac{2}{n}y + 7$$

If we divide by the leading coefficient to make it monic, we get

$$y^3 + \frac{2n^2}{9}y + \frac{7n^3}{9}$$

We want to choose an integer n so that this polynomial has integer coefficients. There are obviously lots of choices, but the smallest one is $n = 3$:

$$y^3 + 2y + 21$$

But really, any integer that's divisible by 3 will work. And all the others won't. ♣

4. Let α be an algebraic number such that $N(\alpha)$ and $\mathrm{Tr}(\alpha)$ are both integers in $\mathbb{Z}$. Must α be an algebraic integer? Either prove it, or give a counterexample.

Solution: No, α might not be an algebraic integer.

The trick to this is to realise that $N(\alpha)$ and $\mathrm{Tr}(\alpha)$ are (up to sign) two of the coefficients of the monic minimal polynomial of α over $\mathbb{Q}$. If there are more than two coefficients, then some of the others might not be integers, and so α won't be an algebraic integer.

For example, let α be a root of the polynomial

$$f(x) = x^3 + x^2 + \frac{1}{2}x + 3$$

Then the norm of α is -3, and the trace of α is -1, but since the monic minimal polynomial of α over $\mathbb{Q}$ doesn't have integer coefficients, α is not an algebraic integer. ♣

5. Consider the ring $A = \mathbb{Z}\left[\frac{1}{2}\right]$. Is A integrally closed?

Solution: Yes, it is integrally closed.

To prove that A is integrally closed, we need to show that if α is an element of the fraction field of A (which is $\mathbb{Q}$), and if α is integral over A, then in fact $\alpha \in A$.

So assume that $\alpha \in \mathbb{Q}$ is integral over A. Then α is the root of a monic polynomial $f(x)$ with coefficients in A. In other words, we have $f(\alpha) = 0$, where:

$$f(x) = x^n + \frac{a_{n-1}}{2^r}x^{n-1} + \ldots + \frac{a_0}{2^r}$$

for integers a_i. (Remember that A is just the ring of dyadic rationals: all rational numbers whose denominators are powers of 2. And the reason I can have the same 2^r in all the coefficients' denominators is that if any of the denominators is smaller than the biggest denominator, I can just multiply its top and bottom by a suitable power of 2 to make it 2^r.)

Plugging in $x = \alpha$ to $f(x) = 0$ and multiplying both sides by 2^r gives:

$$2^r x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$$

where all the a_i are integers. But now α is a rational root of a polynomial with integer coefficients! We know a theorem about that: the Rational Root Theorem. It says that the denominator of α divides evenly into the leading coefficient ... which is 2^r!

So α is a rational number whose denominator is a power of 2. So it's in A. Mission accomplished. ♣

6. Let α be a root of the polynomial $x^3 + 3x + 3$. The ring of integers in the field $\mathbb{Q}(\alpha)$ is $\mathbb{Z}[\alpha]$. (You don't have to prove that.)

Find a basis, over $\mathbb{Z}$, of the ideal $I = (3, \alpha)$. That is, we know that I is isomorphic to $\mathbb{Z}^3$ as an additive group. Your job is to find three elements of I that are a basis for I as an additive group.

Solution: There are lots of bases that work. But the easiest one is $\{\alpha^2, \alpha, 3\}$.

Later in the course, we will develop systematic ways of answering this question. But for now, we have to resort to a trick. Observe that since $\alpha^3 + 3\alpha + 3 = 0$, we have:

$$3 = \alpha(-\alpha^2 - 3) \in (\alpha)$$

In particular, I is really just the ideal (α). So a basis for I can be obtained by taking a basis of $\mathbb{Z}[\alpha]$ and multiplying it by α.

A basis for $\mathbb{Z}[\alpha]$ over $\mathbb{Z}$ is $\{1, \alpha, \alpha^2\}$. Multiplying this by α gives $\{\alpha, \alpha^2, \alpha^3\}$. Now, I suppose I could leave it at that, but I'd rather rewrite it in terms of the original basis of $\mathbb{Z}[\alpha]$, which requires dealing with that α^3:

$$\alpha^3 = -3\alpha - 3$$

So $\{\alpha, \alpha^2, -3\alpha - 3\}$ is a basis, making $\{\alpha^2, \alpha, 3\}$ also a basis. ♣