PMath 441/641 – Homework 1 Solutions

1. Let $M = \mathbb{Z}^3$ and $N = \mathbb{Z}^2$, both $\mathbb{Z}$-modules. Let $\varphi\colon M \to N$ be the $\mathbb{Z}$-module homomorphism $\varphi(a,b,c) = (2a+b, 3b+2c)$. Find generators for the $\mathbb{Z}$-module $\ker\varphi$.

Solution: One possible set of generators is $\{(1,-2,3)\}$. (The only other possible set is $\{(-1,2,-3)\}$.)

If $(a,b,c) \in \ker\varphi$, then $2a+b = 3b+2c = 0$, which means in particular that $b = -2a$, and so $2c = -3b = -6a$, giving $c = 3a$. Thus, the only possible elements of the kernel are elements of the form $(a,-2a,3a)$. It is easy to check that every such element is actually in the kernel:

$$\varphi(a,-2a,-3a) = (2a+(-2a), 3(-2a)+2(3a)) = (0,0)$$

and so we obtain:

$$\ker\varphi = \{(a,-2a,3a) \mid a \in \mathbb{Z}\}$$

which is clearly generated by the single element $(1,-2,3)$. ♣

2. Prove that $\frac{1}{3}(1+10^{1/3}+10^{2/3})$ is an algebraic integer.

Solution: The easiest way to check this is to compute its minimal polynomial. In general, this can be pretty tricky, but in this case it's not too bad. We know that the minimal polynomial of an algebraic number α looks like:

$$p(x) = (x-\alpha)(x-\alpha_1)\dots(x-\alpha_n)$$

where $\alpha,\dots,\alpha_n$ are the Galois conjugates of α. If we set $\alpha = \frac{1}{3}(1+10^{1/3}+10^{2/3})$, then $n = 2$ and:

$$\alpha_1 = \frac{1}{3}(1+\gamma 10^{1/3}+\gamma^2 10^{2/3})$$
$$\alpha_2 = \frac{1}{3}(1+\gamma^2 10^{1/3}+\gamma 10^{2/3})$$

where $\gamma = e^{2\pi i/3}$ is a primitive cube root of unity. Multiplying out the minimal polynomial $p(x)$ then gives:

$$p(x) = x^3 - x^2 - 3x - 3$$

which is monic with integer coefficients, so we're done. ♣

3. Prove that $a = \frac{1+\sqrt{-5}}{2}$ is not integral over $\mathbb{Z}$.

Solution: To show that a is not integral over $\mathbb{Z}$, we just need to show that its monic minimal polynomial does not have integer coefficients. The relevant polynomial is $x^2 - x + \frac{3}{2}$, which obviously does not have integer coefficients. ♣

4. Let $\alpha \in \mathbb{C}$ be a root of $x^3 - x + 1$. Compute the cardinality of the ring $\mathbb{Z}[\alpha]/(\alpha + 2)$. Is the ideal $(\alpha + 2)$ prime?

Solution: The cardinality is 5, and the ideal is prime.

The ring $\mathbb{Z}[\alpha]/(\alpha + 2)$ is isomorphic to the ring $\mathbb{Z}[x]/(x^3 - x + 1, x + 2)$. This, in turn, is isomorphic to the ring $[\mathbb{Z}[x]/(x + 2)]/(x^3 - x + 1)$. The ring inside the brackets is clearly just $\mathbb{Z}$, with the isomorphism taking x to -2. Therefore, we get:

$$\mathbb{Z}[\alpha]/(\alpha + 2) \cong \mathbb{Z}/((-2)^3 - (-2) + 1) = \mathbb{Z}/5\mathbb{Z}$$

Since $\mathbb{Z}/5\mathbb{Z}$ is a domain, the ideal $(\alpha + 2)$ is prime. ♣

5. Let K be a number field of degree d over $\mathbb{Q}$, and let P be a nonzero prime ideal of the ring of integers $\mathcal{O}_K$ of K. Prove that P contains a prime integer p (that is, $p \in \mathbb{Z} \cap P$), and that $\mathcal{O}_K/P$ contains at most p^d elements.

Solution: First note that since P is a nonzero ideal, it contains a nonzero element $\alpha \in P$. The monic minimal polynomial for α over $\mathbb{Q}$ gives an equation like this:

$$\alpha^r + a_{r-1}\alpha^{r-1} + \ldots + a_1\alpha = -a_0$$

where $a_i \in \mathbb{Q}$ and r is a positive integer. (Note that $a_0 \neq 0$ because the minimal polynomial is irreducible.) This means that a_0 is a nonzero integer lying in the ideal P. Since P is prime, it contains at least one prime factor p of a_0.

To compute the number of elements of $\mathcal{O}_K/P$, the idea is that elements of $\mathcal{O}_K$ that are linearly dependent over $\mathbb{Z}$ reduce mod P to elements of $\mathcal{O}_K/P$ that are linearly dependent over $\mathbb{Z}/p\mathbb{Z}$. Since you can't have more than d independent elements in $\mathcal{O}_K$, you can't have more than d independent elements of $\mathcal{O}_K/P$, so the dimension is at most d and you've got at most p^d elements.

Thus, let $V_1, \ldots, V_m$ be any set of vectors in $\mathcal{O}_K/P$, considered as a $(\mathbb{Z}/p\mathbb{Z})$-vector space, and let $v_i \in \mathcal{O}_K$ be an element that reduces to V_i

modulo P. Suppose the elements $\{v_1, \ldots, v_m\}$ are linearly dependent over $\mathbb{Q}$:

$$a_1 v_1 + \ldots a_n v_n = 0$$

for $a_i \in \mathbb{Q}$ not all zero. Then by judicious clearing of denominators, we can ensure that $a_i \in \mathbb{Z}$ for all i, and not all a_i are divisible by p. If we reduce this modulo P, we get a $(\mathbb{Z}/p\mathbb{Z})$-linear dependence relation between the V_i. Since any set of $m > d$ vectors in $\mathcal{O}_K$ is linearly dependent over $\mathbb{Q}$, this shows that any set of $m > d$ elements of $\mathcal{O}_K/P$ are linearly independent over $\mathbb{Z}/p\mathbb{Z}$. The dimension of $\mathcal{O}_K/P$ as a vector space over $\mathbb{Z}/p\mathbb{Z}$ is therefore at most d, so the number of elements is at most p^d, as desired.

Note: Why is $\mathcal{O}_K/P$ a vector space over $\mathbb{Z}/p\mathbb{Z}$? Well, you can add and subtract the elements of $\mathcal{O}_K/P$, it's nonempty, and you can multiply them by elements of $\mathbb{Z}/p\mathbb{Z}$ because $p \in P$: $(a+p\mathbb{Z})(m+P) = am+aP+mp\mathbb{Z}+pP\mathbb{Z} \equiv am \pmod{P}$ because $p \in P$. ♣

6. Prove that the ring of integers of $\mathbb{Q}(\sqrt{33})$ is $\mathbb{Z}\left[\frac{1+\sqrt{33}}{2}\right]$. This is a special case of the general fact that the ring of integers of $\mathbb{Q}(\sqrt{d})$ is (assuming d is squarefree):

$\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ if $d \equiv 1 \pmod 4$
$\mathbb{Z}[\sqrt{d}]$ otherwise

You don't have to do the general case. Just $d = 33$.

In fact, *do not* do the general case. I will take off marks if you do.

Proof: Let's define $\alpha = \frac{1+\sqrt{33}}{2}$, just so we don't have to keep writing out that stuff all the time. Then the monic minimal polynomial for α over $\mathbb{Q}$ is

$$x^2 - x - 8$$

(If you don't see how to do this right away, just compute the Galois conjugate β of α, and multiply out $(x-\alpha)(x-\beta)$.)

In particular, that polynomial has integer coefficients, so $\mathbb{Z}[\alpha]$ is at least contained in the ring of integers.

For the reverse inclusion, let $\gamma = u + v\sqrt{33}$ be an algebraic integer. Then the minimal polynomial for γ over $\mathbb{Q}$ is

$$x^2 + 2ux + (u^2 - 33v^2)$$

Since γ is an algebraic integer, it follows that $2u \in \mathbb{Z}$, so we can write $u = a/2$ for some $a \in \mathbb{Z}$.

But then $a^2/4 - 33v^2 \in \mathbb{Z}$ too, meaning that $33v^2 = b/4$ for some integer b. If we write $v = c/d$ for integers c and d, then d^2 must be a divisor of 4 (and b must be a multiple of 33). By multiplying c and d both by ± 2 if necessary, we can assume that $d = 2$.

Therefore, $a^2 - 33c^2 \in 4\mathbb{Z}$. Reducing modulo 2 gives $a^2 \equiv c^2$, or $a \equiv c$ (modulo 2!). So we can write $a = c + 2k$ for some integer k, and compute:

$$\begin{aligned} \gamma &= \frac{a + c\sqrt{33}}{2} \\ &= \frac{c + 2k + c\sqrt{33}}{2} \\ &= k + c\alpha \end{aligned}$$

which is an element of $\mathbb{Z}[\alpha]$! ♣