Algebra III M3P8, M4P8

Solutions for test 1

1. Using Euclid's algorithm, or otherwise, find a greatest common divisor of 2 and $3 - i$ in the ring $\mathbb{Z}[i]$.

4 marks

The norm of 2 is 4, and the norm of $3 - i$ is 10, so we divide $3 - i$ by 2 with remainder. We need to choose an approximation to $\frac{3-i}{2}$. We can choose 1, because both coordinates of $\frac{3-i}{2} - 1$ are $\leq \frac{1}{2}$. We get $3-i = 2+(1-i)$. Since $(1-i)(1+i) = 2$, we conclude that $\gcd(2, 3 - i) = 1 - i$. (Other correct answers are $-1 + i$, $1 + i$, $-1 - i$.)

2. For each of the following elements of $\mathbb{Z}[\sqrt{2}]$ determine if the element is a unit, an irreducible, or neither:

$$\sqrt{2}, \quad 1 + \sqrt{2}, \quad 2 + \sqrt{2}, \quad 3 + \sqrt{2}, \quad 4 + \sqrt{2}.$$

10 marks, 2 for each part

The norm of $\sqrt{2}$ is -2. As this is not ± 1, we see that $\sqrt{2}$ is not a unit. As -2 cannot be written as a product of two integers different from ± 1, it follows that $\sqrt{2}$ is irreducible.

The norm of $1 + \sqrt{2}$ is -1, so this is a unit.

The norm of $2 + \sqrt{2}$ is 2, so this is an irreducible. (Same arguments as for $\sqrt{2}$.)

The norm of $3 + \sqrt{2}$ is 7, so this is an irreducible. (Same arguments as for $\sqrt{2}$.)

The norm of $4 + \sqrt{2}$ is 14, so we need another idea. We note that the irreducible element $\sqrt{2}$ divides $4 + \sqrt{2}$. The ratio is $1 + 2\sqrt{2}$. The norm of this element is -7, so this is also an irreducible. The conclusion is that $4 + \sqrt{2}$ is neither a unit, nor an irreducible.

3. Let $I \subset \mathbb{Z}[x]$ be the set of polynomials $f(x) = \sum_{i=0}^{n} a_i x^i$ such that $a_i \in \mathbb{Z}$ and a_0, a_1, a_2 are multiples of 3.

6 marks, 2 for each part

(a) Show that I is an ideal in $\mathbb{Z}[x]$.

I is a subgroup stable under multiplication by integers and by x, hence an ideal.

(b) Find $f_1(x), f_2(x) \in \mathbb{Z}[x]$ such that $I = f_1(x)\mathbb{Z}[x] + f_2(x)\mathbb{Z}[x]$.

We can take $f_1(x) = 3$, $f_2(x) = x^3$.

(c) Does there exist $g(x) \in \mathbb{Z}[x]$ such that $I = g(x)\mathbb{Z}[x]$?

No. Since $3 \in I$, the polynomial $g(x)$ is a constant, so it's an integer dividing 3. It can't be ± 1, since $I \neq \mathbb{Z}[x]$. It can't be ± 3, because $x^3 \in I$. This is a contradiction.