MATH453M Homework Solutions Week 10

Nick Inglis
ninglis@math.purdue.edu

4.2.1 a We certainly have $\phi(1) = 1$. let $r = a + b\sqrt{2}$ and $s = c + d\sqrt{2}$. Then

$$\begin{aligned}\phi(r+s) &= \phi\big((a+c) + (b+d)\sqrt{2}\big) = (a+c) - (b+d)\sqrt{2} \\ &= (a - b\sqrt{2}) + (c - d\sqrt{2}) = \phi(r) + \phi(s) \quad \text{and} \\ \phi(rs) &= \phi\big((ab+2cd) + (ad+bc)\sqrt{2}\big) = (ab+2cd) - (ad+bc)\sqrt{2} \\ &= (a - b\sqrt{2})(c - d\sqrt{2}) = \phi(r)\phi(s).\end{aligned}$$

4.2.1 b We have $\phi(\sqrt{3})^2 = (\sqrt{7})^2 = 7 \neq 3 = \phi(3)$ so this is not a homomorphism. If f is such an isomorphism then $f(\sqrt{3}) = a + b\sqrt{7}$ for some $a, b \in \mathbb{Q}$. Now $f(3) = f(1)+f(1)+f(1) = 1+1+1 = 3$ so we must have $3 = f(\sqrt{})^2 = (a+b\sqrt{7})^2 = a^2+2ab\sqrt{7}+7b^2$. Therefore $ab = 0$ since $2ab\sqrt{7} = 3 - a^2 - 7b^2 \in \mathbb{Q}$. Either $b = 0$ in which case $3 = a^2$ which is impossible since $a \in \mathbb{Q}$, or $a = 0$ in which case $3 = 7b^2$, which is impossible since $b \in \mathbb{Q}$. Thus there is no such isomorphism.

4.3.1 a Since $|w| > |z|$ we divide w by z:

$$\frac{w}{z} = \frac{(5-15i)(8-6i)}{8^2+6^2} = \frac{-50-150i}{100} = \frac{-1-3i}{2}.$$

We take $q = -i$ since this this is one of the closest Gaussian integers. This gives $r/z = w/z - q = (-1-i)/2$ and so $r = (-1-i)(8+6i)/2 = -1-7i$. Now

$$\frac{z}{r} = \frac{8+6i)(-1+7i)}{1^2+7^2} = \frac{-50+50i}{50} = -1+i \in \mathbb{Z}[i]$$

so r divides z and hence $\gcd(z, w) = r = -1-7i$ (of course any associate of r is also the gcd, so $-r = 1+7i$, $ir = 7-i$ and $-ir = -7+i$ are equally valid.

4.3.1 b

$$\frac{z}{w} = (4-i)(i-i)1^2 + 1^2 = \frac{3-5i}{2}.$$

We take $q = 1-2i$ since this is one of the closest Gaussian integers. This gives $r/w = z/w - q = (1-i)/2$ so that $r = (1-i)(1+i)/2 = 1$. Therefore $\gcd(z, w) = 1$.

4.3.2 a $6 = 2.3 = (1+i)(1-i)3 = -i(1+i)^2 3$, where $-i$ is a unit, and $1+i$ and 3 are irreducible.

4.3.2 b Let $z = 11 + 7i$. Then

$$z\overline{z} = 121 + 49 = 170 = 2.5.17 = -i(1+i)^2(2+i)(2-i)(4+i)(4-i),$$

$-i$ is a unit and the rest of the factors on the right are irreducibles. By unique factorisation z must be an associate of $(1+i)ab$ where $a \in \{2 \pm i\}$ and $b \in \{4 \pm i\}$. Now let $w = z/(1+i) = (11+7i)(1-i)/2 = (18-4i)/2 = 9-2i$ so w is an associate of ab with a, b as above. Indeed w or $\overline{w}$ is an associate of $(2+i)(4+i)$ or $(2-i)(4+i)$. We have $(2+i)(4+i) = 7+6i$ and $(2-i)(4+i) = 9-2i = w$ so $11+7i = (1+i)(2-i)(4+i)$.

4.3.11 Let $R = \mathbb{Z}[\omega]$. We want to show that given $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ with $|r| < |b|$ such that $a = qb + r$. Equivalently, there exists $q \in R$ with $\left|\frac{a}{b} - q\right| < 1$. It is therefore sufficient to show that given any $z \in \mathbb{C}$ we can find $q \in R$ with $|z - q| < 1$. If we join each element of R to its nearest neighbours in R then this divides $\mathbb{C}$ into equilateral triangles (the nearest elements to 0 are 1, $\omega + 1 = (1 + i\sqrt{3})/2$, ω, -1, $-\omega$ and $1 - \omega$, which form the vertices of a regular hexagon, which comprises 6 equilateral triangles, and this pattern is repeated about every element of R). It follows that every element of $\mathbb{C}$ lies in (or on the border) of such a triangle. But these equilateral triangles have sides of length 1, so every point in the triangle is at distance less than 1 from a vertex.

4.3.13 $2.3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$. All of these elements are irreducible since for each element $|z|^2 \leqslant 9$, but any non-unit in $w \in \mathbb{Z}[i\sqrt{5}]$ has $|w|^2 \geqslant 4$ so any composite w has $|w|^2 \geqslant 16$.

Let $I = \{a + bi\sqrt{5} : a, b \in \mathbb{Z},\ a \equiv b \pmod 2\}$. I claim that I is an ideal (indeed the ideal generated by 2 and $1 + i\sqrt{5}$). Certainly $0 \in I$ and I is closed under addition. Now if $x = a + bi\sqrt{5} \in I$ and $r = c + di\sqrt{5} \in R$ then $xr = (ac - 5bd) + (ad + bc)i\sqrt{5}$ and $(ac - 5bd) - (ad + bc) = (a - b)(c - d) - 6bd$ which is even since $a - b$ is even. Therefore I is an ideal and if $I = \langle g \rangle$ then g divides the irreducible elements 2 and $1 + i\sqrt{5}$. This implies that g is a unit, hence $I = R$ which is nonsense, so I is not a principal ideal.

[In fact any principal ideal domain is a unique factorisation domain.]

4.3.17 For $z = a + bi\sqrt{3} \in \mathbb{Z}[i\sqrt{3}]$ we have $|z|^2 = a^2 + 3b^2 \in \mathbb{N}_0$ and $|wz| = |w||z|$, so any unit must have $1 = |z|^2 = a^2 + 3b^2$ hence $b = 0$ and $a^2 = 1$. Hence the only units are ± 1.

For $r = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ let $r^* = a - b\sqrt{2}$. It is easy to check that $r \mapsto r^*$ is an automorphism of R (an isomorphism from R to itself). Let $N(r) = rr* = (a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2 \in \mathbb{Z}$ so that $N(r) \iff r = 0$. Then $N(rs) = N(r)N(s)$ so if r is a unit then $N(r)$ must be a unit in $\mathbb{Z}$, in other words $N(r) = \pm 1$. Conversely, if $N(r) = \pm 1$ then $1 = \pm N(r) = r(\pm r^*)$ so r is a unit. Therefore the units of $\mathbb{Z}[\sqrt{2}[$ are the elements $a + b\sqrt{2}$ with $a^2 - 2b^2 = \pm 1$.

[In fact there are infinitely many such elements, but each is of the form $\pm(1 + \sqrt{2})^n$ for some $n \in \mathbb{Z}$.]