Exercise 16.24

Submitted by K G Valente

(i) Let R denote the set of Gaussian integers **Z**[i]. Since **Z**[i] is a subset of the complex numbers, which form a ring, we need only check two conditions: $(x + yi) – (u + vi) = (x – u) + (y – v)i \in$ **Z**[i] and $(x + yi)(u + vi) = (xu – yv) + (yu + xv)i \in$ **Z**[i] for all $x + yi, u + vi \in$ **Z**[i]. With these, **Z**[i] is a subring of the complexes, and hence a ring.

(ii) Fix $a = x + yi$ and $b = u + vi$. Then $N(a) = x^2 + y^2$ and $N(b) = u^2 + v^2$. Multiplying gives $N(a)N(b) = (xu)^2 + (yu)^2 + (xv)^2 + (yv)^2$. Now, $ab = (xu - yv) + (yu + xv)i$. Thus $N(ab) = (xu + yv)^2 + (yu + xv)^2 = (xu)^2 + (yu)^2 + (xv)^2 + (yv)^2$. So $N(ab) = N(a)N(b)$.

(iii) Fix $a \in U(R)$. So $ab = 1$ for some $b \in R^*$. With this $N(a)N(b) = N(ab) = N(1) = 1$. Since $N(a)$ and $N(b)$ are integers, we see $N(a)$ must be either 1 or –1.

Now assume $a = x + yi \in R$ with $N(a) = 1$. Consider $b = x – yi \in R$. One checks $ab = x^2 + y^2 = N(a) = 1$.

Finally, if $N(a) = -1$, then consider $(-x) + yi \in R$. Then $ab = -(x)^2 – (y)^2 = - N(a) = 1$. Thus, in either case, $a \in U(R)$.

(iv) By (iii) the only units in **Z**[i] are 1, -1, i, -i. As a multiplicative group, the units are isomorphic to $\mathbf{Z}_4$ as they are generated by i.