TheNumbersBook.com 2010

Stewart: Chapter 3, # 3, 4, 5, 9, 10

Problem 3.3 Let $K = \mathbb{Q}(\zeta)$ where $\zeta = e^{\frac{2\pi i}{p}}$ for a rational prime p. In the ring of integers $\mathbb{Z}[\zeta]$, show that $\alpha \in \mathbb{Z}[\zeta]$ is a unit iff $N_K(\alpha) = \pm 1$.

($\Rightarrow$) If α is a unit, then $\alpha^{-1} \in \mathbb{Z}[\zeta]$. Since $\sigma_i(1) = 1$ for all monomorphisms,

$$\begin{aligned} 1 &= \prod_i \sigma_i(1) \\ &= \prod_i \sigma_i(\alpha\alpha^{-1}) \\ &= \prod_i \sigma_i(\alpha)\sigma_i(\alpha^{-1}) \text{ (σ is a homomorphism)} \\ &= \prod_i \sigma_i(\alpha) \prod_i \sigma_i(\alpha^{-1}) \\ &= N_K(\alpha) N_K(\alpha^{-1}) \end{aligned}$$

Since N_K maps to the integers, the only possibility is $N_K(\alpha) = \pm 1$.

($\Leftarrow$) Since $\mathbb{Z}[\zeta]$ is the ring of integers for K, α is an algebraic integer. Specifically, $\alpha, \sigma(\alpha), \cdots, \sigma_{p-2}(\alpha)$ are all algebraic integers (and so is their product, this we showed). We now see that:

$$\begin{aligned} \pm 1 &= N_K(\alpha) \\ &= \prod_{i=1}^{p-2} \sigma_i(\alpha) \\ &= \alpha \prod_{i=2}^{p-2} \sigma_i(\alpha). \end{aligned}$$

So both α and $\prod_{i=2}^{p-2} \sigma_i(\alpha)$ are units in O_K, as desired. In other words, α times some element $\beta = \prod_{i=2}^{p-2} \sigma_i(\alpha)$ equals the identity (up to reordering of plusses and minuses). Thus, α is a unit. ∎

Problem 3.4 If $\zeta = e^{\frac{2\pi i}{3}}, K = \mathbb{Q}(\zeta)$, prove that the norm of $\alpha \in \mathbb{Z}[\zeta]$ is of the form $\frac{1}{4}(a^2 + 3b^2)$ where a, b are rational integers which are either both even or both odd. Using the result of Exercise 3, deduce that there are precisely six units in $\mathbb{Z}[\zeta]$ and find them all.

The minimal polynomial for K is x^2+x+1 which has the roots ζ, ζ^2. But $\zeta - 2\zeta - 1 = \zeta^2$ so

$$\mathbb{Z}[\zeta] = \{a + b\zeta | a_0, a_1 \in \mathbb{Z}\}$$

and by Theorem 3.5, this is the ring of integers of $\mathbb{Q}(\zeta)$. Notice that $\zeta = -\frac{1}{2} + \frac{\sqrt{3}}{2}$ so we can, equivalently, think of

$$\mathbb{Z}[\zeta] = \{\frac{2a_0 - a_1}{2} + a_1\frac{\sqrt{-3}}{2} | a_0, a_1 \in \mathbb{Z}\}$$

where the monomorphisms are the identity and $\sqrt{-3} \to -\sqrt{-3}$. Taking the norm yields the desired form:

$$\begin{aligned} N_K(\alpha) &= (\frac{2a_0 - a_1}{2} + a_1\frac{\sqrt{-3}}{2})(\frac{2a_0 - a_1}{2} - a_1\frac{\sqrt{-3}}{2}) \\ &= \frac{(2a_0 - a_1)^2}{4} + \frac{a_1^2}{4}3 \\ &= \frac{1}{4}(a^2 + 3b^2) \text{ (for } a, b \text{ rational integers)} \end{aligned}$$

where $a = 2a_0 - a_1$ and $b = a_1$. Note that if $b = a_1$ is even then so is a. Similarly, if $b = a_1$ is odd, then so is a. Thus, a and b are both even or both odd.

From 3.3, we know that α is a unit iff $N_K(\alpha) = \frac{1}{4}(a^2 + 3b^2) = 1$. Rewriting, we have $a^2 + 3b^2 = 4$ which has exactly six solutions: $(1,1)$, $(2,0)$, $(-1,-1)$, $(-1,1)$, $(1,-1)$, $(-2,0)$. In other words, the six units are

$$\pm\frac{1}{2} \pm \frac{1}{2}\sqrt{-3}, \pm 1$$

■

Problem 3.5 If $\zeta = e^{\frac{2\pi i}{5}}, K = \mathbb{Q}(\zeta)$, prove that the norm of $\alpha \in \mathbb{Z}[\zeta]$ is of the form $\frac{1}{4}(a^2 - 5b^2)$ where a, b are rational integers. (Hint: in calculating $N(\alpha)$, firsct calculate $\sigma_1(\alpha)\sigma_4(\alpha)$ where $\sigma_i(\zeta) = \zeta^i$. Show that this is of the form $q + r\theta + s\phi$ where q, r, s are rational integers, $\theta = \zeta + \zeta^4, \phi = \zeta^2 + \zeta^3$. In the same way, establish $\sigma_2(\alpha)\sigma_3(\alpha) = q + s\theta + r\phi$.) Using Exercise 3, prove that $\mathbb{Z}[\zeta]$ has an infinite number of units.

By Theorem 3.5, $\mathbb{Z}[\zeta] = \{a_1 + a_2\zeta + a_3\zeta^2 + a_4\zeta^3\}$ is the ring of integers with the integral basis $\{1, \zeta, \zeta^2, \zeta^3\}$.. Define $\sigma_i(\zeta) = \zeta^i$. Then

$$
\begin{aligned}
\sigma_1(\alpha)\sigma_4(\alpha) &= (a_1 + a_2\zeta + a_3\zeta^2 + a_4\zeta^3)\sigma_4(a_1 + a_2\zeta + a_3\zeta^2 + a_4\zeta^3) \\
&= (a_1 + a_2\zeta + a_3\zeta^2 + a_4\zeta^3)(a_1 + a_2\sigma_4(\zeta) + a_3\sigma_4(\zeta)^2 + a_4\sigma_4(\zeta)^3) \\
&= (a_1 + a_2\zeta + a_3\zeta^2 + a_4\zeta^3)(a_1 + a_2\zeta^4 + a_3\zeta^8 + a_4\zeta^{12}) \\
&= a_1^2 + a_1a_2\zeta + a_1a_3\zeta^2 + a_1a_4\zeta^3 + a_1a_2\zeta^4 + a_2^2\zeta^5 + a_2a_3\zeta^6 + a_2a_4\zeta^7 + a_1a_3\zeta^8 + a_2 \\
&+ a_3\zeta^9 + a_3^2\zeta^10 + a_3a_4\zeta^11 + a_1a_4\zeta^12 + a_2a_4\zeta^13 + a_3a_4\zeta^14 + a_4^2\zeta^15 \\
&= a_1^2 + a_1a_2\zeta + a_1a_3\zeta^2 + a_1a_4\zeta^3 + a_1a_2\zeta^4 + a_2^2 + a_2a_3\zeta + a_2a_4\zeta^2 + a_1a_3\zeta^3 + a_2a_3\zeta^4 \\
&+ a_3^2 + a_3a_4\zeta + a_1a_4\zeta^2 + a_2a_4\zeta^3 + a_3a_4\zeta^4 + a_4^2 \\
&= (a_1^2 + a_2^2 + a_3^2 + a_4^2) + (a_1a_2 + a_2a_3 + a_3a_4)(\zeta + \zeta^4) + (a_1a_3 + a_1a_4 + a_2a_4)(\zeta^2 + \zeta^3) \\
&= q + r\theta + s\phi
\end{aligned}
$$

where q, r, s are rational integers,$\theta = \zeta_1 + \zeta_4$ and $\phi = \zeta_2 + \zeta_3$. Similarly,

$$
\begin{aligned}
\sigma_2(\alpha)\sigma_3(\alpha) &= \sigma_2(a_1 + a_2\zeta + a_3\zeta^2 + a_4\zeta^3)\sigma_3(a_1 + a_2\zeta + a_3\zeta^2 + a_4\zeta^3) \\
&= (a_1 + a_2\zeta^2 + a_3\zeta^4 + a_4\zeta^6)(a_1 + a_2\zeta^3 + a_3\zeta^6 + a_4\zeta^9) \\
&= a_1^2 + a_1a_2\zeta^2 + a_1a_2\zeta^3 + a_1a_3\zeta^4 + a_2^2\zeta^5 + a_1a_3\zeta^6 + a_1a_4\zeta^6 + a_2a_3\zeta^7 + a_2a_3\zeta^8 \\
&+ a_1a_4\zeta^9 + a_2a_4\zeta^9 + a_3^2\zeta^{10} + a_2a_4\zeta^{11} + a_3a_4\zeta^{12} + a_3a_4\zeta^{13} + a_4^2\zeta^{15} \\
&= a_1^2 + a_1a_2\zeta^2 + a_1a_2\zeta^3 + a_1a_3\zeta^4 + a_2^2 + a_1a_3\zeta + a_1a_4\zeta + a_2a_3\zeta^2 + a_2a_3\zeta^3 \\
&+ a_1a_4\zeta^4 + a_2a_4\zeta^4 + a_3^2 + a_2a_4\zeta + a_3a_4\zeta^2 + a_3a_4\zeta^3 + a_4^2 \\
&= (a_1^2 + a_2^2 + a_3^2 + a_4^2) + (a_1a_3 + a_1a_4 + a_2a_4)(\zeta + \zeta^4) + (a_1a_2 + a_2a_3 + a_3a_4)(\zeta^2 + \zeta^3) \\
&= q + s\theta + r\phi
\end{aligned}
$$

where q, s, r are rational integers. We know that

$$
\begin{aligned}
\zeta &= \frac{1}{4}(-1 + \sqrt{5}) + \sqrt{\frac{5}{8} + \frac{\sqrt{5}}{8}} \\
\zeta^2 &= \frac{1}{4}(-1 - \sqrt{5})\sqrt{\frac{5}{8} - \frac{\sqrt{5}}{8}} \\
\zeta^3 &= \frac{1}{4}(-1 - \sqrt{5}) - \sqrt{\frac{5}{8} - \frac{\sqrt{5}}{8}} \\
\zeta^4 &= \frac{1}{4}(-1 + \sqrt{5}) - \sqrt{\frac{5}{8} + \frac{\sqrt{5}}{8}}
\end{aligned}
$$

Thus, we have that $\theta = \zeta + \zeta^4 = \frac{1}{2}(-1 + \sqrt{5})$ and $\phi = \zeta^2 + \zeta^3 = \frac{1}{2}(-1 - \sqrt{5})$. We can finally calculate the norm:

$$\begin{aligned}
N_K(\alpha) &= \sigma_1(\alpha)\sigma_4(\alpha)\sigma_2(\alpha)\sigma_3(\alpha) \\
&= (q + r\theta + s\phi)(q + s\theta + r\phi) \\
&= q^2 + qs\theta + qr\phi + rq\theta + rs\theta^2 + r^2\theta\phi + sq\phi + s^2\theta\phi + sr\phi^2 \\
&= q^2 + qs(\theta + \phi) + qr(\phi + \theta) + rs(\theta^2 + \phi^2) + (r^2 + s^2)\theta\phi \\
&= q^2 + qs(-1) + qr(-1) + rs(\frac{1}{2}(3 - \sqrt{5}) + \frac{1}{2}(3 + \sqrt{5})) + \frac{1}{4}(r^2 + s^2)(1 - 5) \\
&= \frac{1}{4}(4q^2 - 4qs - 4qr + 12rs + r^2 + s^2 - 5r^2) - \frac{1}{4}5s^2 \\
&= \frac{1}{4}(a^2 - 5b^2)
\end{aligned}$$

where a, b are rational integers.

Finally, by Problem 3.3, α is a unit iff $N_K(\alpha) = \frac{1}{4}(a^2 - 5b^2) = \pm 1$. Rewriting yields $a^2 - 5b^2 = \pm 4$. This is a famous Diophantine equation that has infinitely many solutions. Thus, there is an infinite number of units. ■

Problem 3.9 Suppose p is a rational prime and $\zeta = e^{\frac{2\pi i}{p}}$. Given that the group of non-zero elements of Z_p is cyclic (see Appendix 1, Prop 6 for a proof) show that there exists a monomorphism $\sigma : Q(\zeta) \to C$ such that σ^{p-1} is the identity and all monomorphisms from $Q(\zeta)$ to C are of the form $\sigma^i (1 \leq i \leq p-1)$. If $p - 1 = kr$, define $c_k(\alpha) = \alpha\sigma^r(\alpha)\sigma^{2r}(\alpha)\cdots\sigma^{(k-1)r}(\alpha)$. Show

$$N(\alpha) = c_k(\alpha) \cdot \sigma c_k(\alpha) \cdots \sigma^{r-1} c_k(\alpha).$$

Prove every element of $Q(\zeta)$ is uniquely of the form $\sum_{i=1}^{p-1} a_i \zeta^i$, and by demonstrating that $\sigma^r(c_k(\alpha)) = c_k(\alpha)$, deduce that $c_k(\alpha) = b_1\eta_1 + \cdots + b_k\eta_r$, where

$$\nu_1 = \zeta + \sigma^r(\zeta) + \sigma^{2r}(\zeta) + \cdots + \sigma^{(k-1)r}(\zeta)$$

and $\eta_{i+1} = \sigma^i(\eta_1)$.
Interpret these results in the case $p = 5, k = r = 2$, by showing that the residue class of 2 is a generator of the multiplicative group of non-zero elements of Z_5. Demonstrate that $c_2(\alpha)$ is of the form $b_1\nu_1 + b_2\nu_2$ where $\nu_1 = \zeta + \zeta^4, \nu_2 = \zeta^2 + \zeta^3$. Calculate the norms of the following elements in $Q(\zeta)$: (i) $\zeta + 2\zeta^2$, (ii) $\zeta + \zeta^4$, (iii) $15\zeta + 15\zeta^4$, (iv) $\zeta + \zeta^2 + \zeta^3 + \zeta^4$.

Define $\sigma : \mathbb{Q}(\zeta) \to \mathbb{C}$ by

$$\sigma(\zeta) = \zeta^{p-1}$$

Note that $\sigma^i(\zeta) = \sigma(\zeta)^i = \zeta^{(p-1)^i} = e^{\frac{2\pi(p-1)^i}{p}}$. The term $\frac{(p-1)^i}{p}$ has the form $(p-1)^i(\text{mod} p)$, which is the general form of $\mathbb{Z}_p$. Thus, what the monomorphism σ^i does can be explained using $\mathbb{Z}_p$.Specifically, since

$$\gcd(p, p-1) = 1$$

$p-1$ is a generator for $\mathbb{Z}_p$ and so $(p-1)^i \in \mathbb{Z}_p^\times$ for $i = 1, \cdots, p-1$. This proves that σ^i maps ζ to every power of ζ. Specifically, $(p-1)^{p-1} = 1(\text{mod} p)$ because $|\mathbb{Z}_p| = \phi(p) = p-1$ and so $(p-1)^{p-1}$ is the identity. This proves that σ^{p-1} is the identity monomorphism.

We now show that $N(\alpha) = c_k(\alpha)\sigma(c_k(\alpha)) \cdots \sigma^{r-1}(c_k(\alpha))$. First, using the generic definition of norm, we have

$$
\begin{aligned}
N_K(\alpha) &= \prod_{i=1}^{p-1} \sigma^i(\alpha) \\
&= \alpha \prod_{i=1}^{p-2} \sigma^i(\alpha) \\
&= \alpha\sigma^{1+2+\cdots+p-2}(\alpha) \\
&= \alpha\sigma^{(p-1)(p-2)/2}(\alpha) \text{ (1)}
\end{aligned}
$$

Now let us write out each $c_k(\alpha)$:

$$
\begin{aligned}
c_k(\alpha) &= \alpha\sigma^r(\alpha)\sigma^{2r}(\alpha) \cdots \sigma^{(k-1)r}(\alpha) \\
\sigma c_k(\alpha) &= \sigma(\alpha)\sigma^{r+1}(\alpha)\sigma^{2r+1}(\alpha) \cdots \sigma^{(k-1)r+1}(\alpha) \\
&\cdots \\
\sigma^{r-1} c_k(\alpha) &= \sigma^{r-1}(\alpha)\sigma^{2r-1}(\alpha)\sigma^{3r-1}(\alpha) \cdots \sigma^{(k-1)r+r-1}(\alpha)
\end{aligned}
$$

Now note something remarkable: if we count the powers of σ in a zig-zag fashion (that is: go down, then move up, and count down again), we see that the powers are simply adding $1, 2, 3, \cdots$ all the way up to $(k-1)r + r - 1 = kr - 1$. Thus,

$$
\begin{aligned}
c_k(\alpha)\sigma c_k(\alpha) \cdots \sigma^{r-1} c_k(\alpha) &= \alpha\sigma^{1+2+\cdots+kr-1}(\alpha) \\
&= \alpha\sigma^{kr(kr-1)/2} \\
&= \alpha\sigma^{(p-1)(p-2)/2} \\
&= N(\alpha) \text{ (from above)}
\end{aligned}
$$

as desired.

We now show that any element in $\mathbb{Q}(\zeta)$ can be written uniquely in the form $\sum_{i=1}^{p-1} a_i \zeta^i$. This follows from the definition of $\mathbb{Q}(\zeta)$ as a vector space. Now note that

$$
\begin{aligned}
\sigma^r(c_k(\alpha)) &= \sigma^r(\alpha\sigma^r(\alpha)\sigma^{2r}(\alpha) \cdots \sigma^{(k-1)r}(\alpha)) \\
&= \sigma^r(\alpha)\sigma^{2r}(\alpha)\sigma^{3r}(\alpha) \cdots \sigma^{(k-2)r+r}\sigma^{kr}(\alpha) \\
&= \sigma^r(\alpha)\sigma^{2r}(\alpha)\sigma^{3r}(\alpha) \cdots \sigma^{(k-2)r+r}\alpha \text{ (since } kr = p-1) \\
&= c_k(\alpha) \text{ (since } \sigma \text{ commutes)}
\end{aligned}
$$

Thus, we see that σ^r fixes $c_k(\alpha)$. We now use this result to show that

$$c_k(\alpha) = b_1 v_1 + \cdots + b_n v_n$$

First,

$$\begin{aligned}
c_k(\alpha) &= \sum_{i=1}^{p-1} a_i \zeta^i \\
\sigma^r(c_k(\alpha)) &= \sigma^r(\sum_{i=1}^{p-1} a_i \zeta^i) \\
c_k(\alpha) &= \sum_{i=1}^{p-1} a_i \sigma^r(\zeta^i) \text{ } (\sigma^r \text{ fixes } c_k(\alpha)) \\
&= \sum_{i=1}^{p-1} a_i \sigma^{ri}(\zeta) \\
&= a_1\sigma^r(\zeta) + a_2\sigma^{2r}(\zeta) + \cdots + a_{p-1}\sigma^{(p-1)r}(\zeta) \\
&= a_{p-1}\zeta + a_1\sigma^r(\zeta) + \cdots + a_{p-2}\sigma^{(p-2)r}(\zeta) \text{ (since } \sigma^{p-1} = 1) \\
&= \underbrace{(\zeta + \cdots + \zeta)}_{a_{p-1} \text{ terms}} + \underbrace{(\sigma^r(\zeta) + \cdots + \sigma^r(\zeta))}_{a_1 \text{ terms}} + \cdots + \underbrace{(\sigma^{(p-2)r}(\zeta) + \cdots + \sigma^{(p-2)r}(\zeta))}_{a_{p-2} \text{ terms}} \\
&= (\zeta + \sigma^r(\zeta) \cdots + \sigma^{(p-2)r}(\zeta)) + \cdots + (\zeta + \sigma^r(\zeta) \cdots + \sigma^{(p-2)r}(\zeta))
\end{aligned}$$

Now let $\eta_1 = \zeta + \sigma^r(\zeta) \cdots + \sigma^{(p-2)r}(\zeta)$ and since $\sigma(\zeta + \sigma^r(\zeta) + \cdots + \sigma^{(p-2)r}(\zeta)) = \zeta + \sigma^r(\zeta) + \cdots + \sigma^{(p-2)r}(\zeta)$, we have that

$$\begin{aligned}
c_k(\alpha) &= (\zeta + \sigma^r(\zeta) \cdots + \sigma^{(p-2)r}(\zeta)) + \cdots + ((\zeta + \sigma^r(\zeta) \cdots + \sigma^{(p-2)r}(\zeta))) \\
&= b_1\eta_1 + b_2\sigma(\eta_1) + b_3\sigma^2(\eta_1) + \cdots + b_r\sigma^{r-1}(\eta_1)
\end{aligned}$$

The above form gives precisely:

$$c_k(\alpha) = b_1\eta_1 + b_2\eta_2 + \cdots + b_r\eta_r$$

We will now interpret these results in the case $p = 5$ and $k = 2 = r$. Note that the residue class of 2 is a generator for $\mathbb{Z}_5^\times$ since $2, 2^2 = 4, 2^3 = 3, 2^4 = 1$. In this case, we define $\sigma(\zeta) = \zeta^2$ and this generates all 5-roots of unity. Using the notation above, we see that $c_(\alpha) = b_1 v_1 + b_2 v_2$ where $v_1 = \zeta + \sigma^2(\zeta) = \zeta + \zeta^4$ and $v_2 = \sigma(\zeta) + \sigma(\zeta^4) = \zeta^2 + \zeta^3$.

We now calculate a couple of norms. To simplify our work, we will refer to the following table:

$$\begin{aligned}
\sigma(\zeta) &= \zeta^2 \\
\sigma(\zeta^2) &= \zeta^4 \\
\sigma(\zeta^3) &= \zeta \\
\sigma(\zeta^4) &= \zeta^3
\end{aligned}$$

One more thing, the identity $\Phi(\zeta) = \zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0$ will prove useful.

(i) To calculate norm of $\zeta + 2\zeta^2$, we first calculate $c_2(\zeta + 2\zeta^2)$:

$$c_2(\zeta + 2\zeta^2) = (\zeta + 2\zeta^2)\sigma^2(\zeta + 2\zeta^2) = (\zeta + 2\zeta^2)(\zeta^4 + 2\zeta^3) = 5 + 2\zeta^4 + 2\zeta$$

Thus,

$$\begin{aligned} N(\zeta + 2\zeta^2) &= c_2(\alpha)\sigma(c_2(\alpha)) \\ &= (5 + 2\zeta^4 + 2\zeta)\sigma(5 + 2\zeta^4 + 2\zeta) \\ &= (5 + 2\zeta^4 + 2\zeta)(5 + 2\zeta^3 + 2\zeta^2) \\ &= 25 + 14\zeta + 14\zeta^2 + 14\zeta^3 + 14\zeta^4 \\ &= 25 - 14 \\ &= 11 \end{aligned}$$

(ii) To calculate norm of $\zeta + \zeta^4$, we first calculate $c_2(\zeta + \zeta^4)$:

$$c_2(\zeta + \zeta^4) = (\zeta + \zeta^4)\sigma^2(\zeta + \zeta^4) = (\zeta + \zeta^4)(\zeta^4 + \zeta) = 2 + \zeta^2 + \zeta^3$$

Thus,

$$\begin{aligned} N(\zeta + \zeta^4) &= c_2(\alpha)\sigma(c_2(\alpha)) \\ &= (2 + \zeta^2 + \zeta^3)\sigma(2 + \zeta^2 + \zeta^3) \\ &= (2 + \zeta^2 + \zeta^3)(2 + \zeta^4 + \zeta) \\ &= 4 + 3\zeta + 3\zeta^2 + 3\zeta^3 + 3\zeta^4 \\ &= 4 - 3 \\ &= 1 \end{aligned}$$

(iii) To calculate norm of $15\zeta + 15\zeta^4$, note that $c_2(15) = 15^2$. Thus,

$$\begin{aligned} N(15\zeta + 15\zeta^4) &= N(15)N(\zeta + \zeta^4) \\ &= 15^4(4 + 3\zeta + 3\zeta^2 + 3\zeta^4) \\ &= 15^4 \end{aligned}$$

(iv) Note that $\zeta + \zeta^2 + \zeta^3 + \zeta^4 + 1 = 0$ (cyclotomic polynomial) so $\zeta + \zeta^2 + \zeta^3 + \zeta^4 = -1$. Thus,

$$N(\zeta + \zeta^2 + \zeta^3 + \zeta^4) = c_2(-1)\sigma(c_2(-1)) = -1(-1)(-1)(-1) = 1$$

∎

Problem 3.10 In $Z[\sqrt{-5}]$, prove 6 factorizes in two ways as

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

Verify that $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ have no proper factors in $Z[\sqrt{-5}]$. (HINT: Take norms and note that if γ factorizes as $\gamma = \alpha\beta$, then $N(\gamma) = N(\alpha)N(\beta)$ is a factorization of rational integers.) Deduce that it is possible in $Z[\sqrt{-5}]$ for 2 to have no proper factors, yet 2 divides a product $\alpha\beta$ without dividing either α or β.

Suppose $6 = \alpha\beta$ for $\alpha = a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ and $\beta = c + d\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$. Then,

$$\begin{aligned} N_K(6) &= N_K(\alpha\beta) \\ 36 &= N_K(\alpha)N_K(\beta) \\ 36 &= (a^2 + 5b^2)(c^2 + 5d^2) \end{aligned}$$

The possible factorizations of 36 are $36 \times 1, 6 \times 6, 9 \times 4, 3 \times 12$ and 2×18 (up to reordering). It is easy to see that both 2×18 and 3×12 are impossible factorization as there is no way to express 2 (or 3)in the form $a^2 + 5b^2$. Now consider 36×1. Then, $a = \pm 6, b = 0, c = \pm 1, d = 0$. For 6×6, $a = b = \pm 1, c = d = \pm 1$. For 9×4, $a = \pm 2, b = \pm 1, c = \pm 2, d = 0$. Testing all these possibilities on $6 = (a + b\sqrt{-5})(c + d\sqrt{-5})$ and noting that 6 has no factor of $\sqrt{-5}$, we dedude the only solutions: $a = 2, b = 0, c = 3, d = 0$ and $a = b = 1, c = 1, d = -1$. Thus,

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

We now show that 2 has no proper factors. Suppose $2 = \alpha\beta$, then $N_K(2) = 4 = N_K(\alpha)N_K(\beta) = (a^2 + 5b^2)(c^2 + 5d^2)$. The only possible values are $a = \pm 2, b = 0, c = \pm 1, d = 0$, which, when plugged back into the general form of an element, yields only 2 (plus or minus that). Thus, 2 has no proper factors. Similarly, $N_K(3) = 9 = N_K(\alpha)N_K(\beta) = (a^2 + 5b^2)(c^2 + 5d^2)$. The possible factorizations are 9×1 and 3×3. Plugging in the respective a, b, c, d values returns 3 (plus or minus). Thus, 3 has no proper factors.
Now consider $1 + \sqrt{-5}$. Then $N_K(1 + \sqrt{-5}) = 6$ and only $6 \cdot 1$ is a possibility (since 2×3 has 2 which can't be expressed by $a^2 + 5b^2$). Thus, $a^2 + 5b^2 = 6, c^2 + 5b^2 = 1$ and so $a = b = \pm 1, c = \pm 1$. These possibilities, when plugged into the general form for an element, return $1 + \sqrt{-5}$. Thus, $1 + \sqrt{-5}$ has no proper factors. Similarly, $N_K(1 - \sqrt{-5}) = 6$ and the same cases follow. Thus, $1 - \sqrt{-5}$ has no proper factors.

Finally, note that $2 | 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ but $2 \not| (1 + \sqrt{-5})$ and $2 \not| (1 - \sqrt{-5}$.

$\blacksquare$