MATH 5590H HOMEWORK 11

BRENDAN WHITAKER

Exercise 8.2.5. *Let R be the quadratic integer ring $\mathbb{Z}[\sqrt{-5}]$. Define the ideals $I_2 = (2, 1 + \sqrt{-5})$, $I_3 = (3, 2 + \sqrt{-5})$, and $I_3' = (3, 2 - \sqrt{-5})$.*

(a) *Prove that these are all nonprincipal ideals in R.*
Proof. Suppose $I_2 = (a + b\sqrt{-5})$, with $a, b \in \mathbb{Z}$ was principal. Then $\exists \alpha, \beta \in R$ such that

$$\begin{aligned} 2 &= \alpha(a + b\sqrt{-5}), \\ 1 + \sqrt{-5} &= \beta(a + b\sqrt{-5}). \end{aligned} \tag{1}$$

Then we have

$$\begin{aligned} 4 &= N(\alpha)(a^2 + 5b^2), \\ 6 &= N(\beta)(a^2 + 5b^2). \end{aligned} \tag{2}$$

Then $(a^2 + 5b^2) = 1, 2,$ or 4. It cannot be 4, since there is no integer value for $N(\beta)$ s.t. $6 = 4N(\beta)$. It cannot be 2 since there are no integer solutions to $2 = a^2 + 5b^2$. And if it is 1, then we must have $a = \pm 1$, and $b = 0$, so $I_2 = (\pm 1) = R$. Then 1 is in I_2, so $\exists \gamma, \delta \in R$ s.t. $2\gamma + \delta(1 + \sqrt{-5}) = 1$. But that would give us

$$\begin{aligned} 2\gamma(1 - \sqrt{-5}) + 6\delta &= 1 - \sqrt{-5}, \\ 2(\gamma(1 - \sqrt{-5} + 3\delta) &= 1 - \sqrt{-5}, \end{aligned} \tag{3}$$

which is impossible, since $(1 - \sqrt{-5})$ is not divisible by 2. Thus I_2 cannot be principal. □

We make a similar argument for I_3.
Proof. Suppose $I_3 = (a + b\sqrt{-5})$, with $a, b \in \mathbb{Z}$ was principal. Then $\exists \alpha, \beta \in R$ such that

$$\begin{aligned} 3 &= \alpha(a + b\sqrt{-5}), \\ 2 + \sqrt{-5} &= \beta(a + b\sqrt{-5}). \end{aligned} \tag{4}$$

Then we have

$$\begin{aligned} 9 &= N(\alpha)(a^2 + 5b^2), \\ 9 &= N(\beta)(a^2 + 5b^2). \end{aligned} \tag{5}$$

So $a^2 + 5b^2 = 1$, 3, or 9. If it is 9, then then $N(\alpha) = 1$, and thus $\alpha = \pm 1$, and then $(a + b\sqrt{-5}) = \pm 3$, which is impossible, since $2 + \sqrt{-5}$ is not divisible by 3. If $a^2 + 5b^2 = 3$, then since there are not integer solutions to $a^2 + 5b^2 = 3$, we have a contradiction. And if $a^2 + 5b^2 = 1$, then we have that $(a + b\sqrt{-5}) = \pm 1$, so $I_3 = (\pm 1) = R$. Then we must have $\delta, \gamma \in R$ s.t. $3\gamma + \delta(2 + \sqrt{-5}) = 1$. But then we have

$$\begin{aligned} 3\gamma(2 - \sqrt{-5}) + 9\delta &= (2 - \sqrt{-5}), \\ 3(\gamma(2 - \sqrt{-5}) + 3\delta) &= (2 - \sqrt{-5}), \end{aligned} \tag{6}$$

which is impossible because $(2 - \sqrt{-5})$ is not divisible by 3. Thus I_3 cannot be principal. □

Again, we make a similar argument for I_3'.
Proof. Following precisely the same argument as in the above proof for I_3, but multiplying instead by $(2 + \sqrt{-5})$ in equation (6), we have that I_3' cannot be principal. □

(b) *Prove that the product of two nonprincipal ideals can be principal by showing that $I_2^2 = (2)$ in R.*

Date: AU17.

Proof. Let α, β be arbitrary elements of I_2, where $\alpha = 2a+(1+\sqrt{-5})b$, and $\beta = 2c+(1+\sqrt{-5})d$, for $a, b, c, d \in \mathbb{Z}$. Then any element of I_2^2 is of the form

$$\begin{aligned}\alpha\beta &= (2a + (1+\sqrt{-5})b)(2c + (1+\sqrt{-5})d)\\ &= 4ac + 2ad(1+\sqrt{-5}) + 2cb(1+\sqrt{-5}) + bd(1 + 2\sqrt{-5} + -5)\\ &= 4ac + 2ad + 2ad\sqrt{-5} + 2cb + 2cb\sqrt{-5} + 2bd\sqrt{-5} - 4bd \qquad (7)\\ &= 2(2ac + ad + ad\sqrt{-5} + cb + cb\sqrt{-5} + bd\sqrt{-5} - 2bd)\\ &= 2((2ac + ad + cb - 2bd) + (ad + cb + bd)\sqrt{-5}),\end{aligned}$$

and since a, b, c, d are integers, we know that $\alpha\beta$ is of the form $2r$ for $r \in R$. Thus $I_2^2 = (2)$, since for appropriate choice of a, b, c, d we may let r be any element of R. Hence I_2^2 is a principal ideal. ☐

(c) *Prove similarly that $I_2 I_3 = (1-\sqrt{-5})$, and $I_2 I_3' = (1+\sqrt{-5})$. Conclude that the principal ideal (6) is the product of 4 ideals: $(6) = I_2^2 I_3 I_3'$.*

Proof. We show that $1-\sqrt{-5}$ can be written as the product of the generators of I_2 and I_3, respectively, to show $(1-\sqrt{-5}) \subset I_2 I_3$, and we show each of the generators of I_2 and I_3 are generated by $1-\sqrt{-5}$ to show $I_2 I_3 \subset (1-\sqrt{-5})$. Note

$$1 - \sqrt{-5} = 3 - (2 + \sqrt{-5}), \qquad (8)$$

so $(1-\sqrt{-5}) \subset I_2 I_3$, let $\alpha = 1-\sqrt{-5}$, and also note

$$\begin{aligned}I_2 I_3 &= (2, 1+\sqrt{-5})(3, 2+\sqrt{-5}) = (6, 4+2\sqrt{-5}, 3+3\sqrt{-5}, -3+3\sqrt{-5}),\\ 6 &= \alpha\overline{\alpha},\\ 4 + 2\sqrt{-5} &= -\alpha^2, \qquad (9)\\ 3 + 3\sqrt{-5} &= \alpha(-2+\sqrt{-5}),\\ -3 + 3\sqrt{-5} &= -3\alpha.\end{aligned}$$

Thus each of the generators of $I_2 I_3$ is in $(1-\sqrt{-5})$, so $I_2 I_3 \subset (1-\sqrt{-5}) \Rightarrow I_2 I_3 = (1-\sqrt{-5})$. The fact that $I_2 I_3' = (1+\sqrt{-5})$ follows from precisely the same argument by taking complex conjugates. Now $I_2^2 I_3 I_3' = I_2 I_3 \cdot I_2 I_3' = (1-\sqrt{-5})(1+\sqrt{-5}) = (6)$. ☐

Exercise 8.3.8. *Let R, I_2, I_3, I_3' be as defined in Exercise 8.2.5. Again, let $\alpha = 1-\sqrt{-5}$.*

(a) *Prove that $2, 3, \alpha, \overline{\alpha}$ are all irreducibles in R, none of which are associate, and that $6 = 2\cdot 3 = \cdot\alpha\overline{\alpha}$ are two distinct factorizations of 6 into irreducibles in R.*

Proof. We use the fact that R is an integral domain. Let $2 = r(a+b\sqrt{-5})$, where $r, (a+b\sqrt{-5}) \in R$. Then taking the associated field norm, we have

$$4 = N(r)(a^2 + 5b^2), \qquad (10)$$

and since $a^2 + 5b^2$ is a positive integer, it must be 1, 2, or 4. If it is 4, then $N(r) = 1 \Rightarrow r = \pm 1 \Rightarrow r$ is a unit, so in this case 2 is irreducible. Suppose $a^2 + 5b^2 = 2$. This is impossible as the equation is insoluble in integers. So let $a^2 + 5b^2 = 1$. Then $a = \pm 1$, $b = 0$, and thus $(a + b\sqrt{-5})$ is a unit, so again 2 is irreducible. Note that 3 is irreducible by precisely the same argument, using the equation $9 = N(r)(a^2 + 5b^2)$, since $3 = a^2 + 5b^2$ is not soluble in integers, and the factors of 9 are $1, 3, 9$.

Now let $\alpha = r(a + b\sqrt{-5})$. Taking norms we have

$$6 = N(r)(a^2 + 5b^2), \qquad (11)$$

where the possible values for $a^2 + 5b^2$ are 1, 2, 3, or 6. We immediately have that α is irreducible in the case where the value is 1, since then $(a + b\sqrt{-5}) = \pm 1$, a unit, or 6, since then r is a unit. And the other cases, where $a^2 + 5b^2$ is 2 or 3, follow directly from the insolubility in integers of the equations mentioned above. Thus α is irreducible, and $\overline{\alpha}$'s irreducibility follows from precisely the same argument, since $\alpha, \overline{\alpha}$ have the same norm. Note 2 and 3 could not possibly be associates with each other or the other two elements in question, since they differ in norm. It remains to be shown that $\alpha, \overline{\alpha}$ are not associate. Since units in R must have norm 1, and this implies $b = 0$ for any element of the form $a + b\sqrt{-5}$, we know all units ± 1. And clearly $-\alpha \neq \overline{\alpha}$, so they are not associate. $\square$

(b) *Prove that I_2, I_3, I_3' are prime ideals.*

Proof. Note we proved these are all nonprincipal ideals in a previous exercise. Let $a+b\sqrt{-5} \in R$, then we have

$$a + b\sqrt{-5} \equiv a - b \equiv 0 \text{ or } 1 \mod I_2 \tag{12}$$

since $1 + \sqrt{-5} \equiv 0 \mod I_2$, and $2 \equiv 0 \mod I_2$. So we have at most 2 elements. Thus we must have $R/I_2 \cong \mathbb{F}_2$. And since $\mathbb{F}_2$ is an integral domain, we have that I_2 must be prime, since if R is commutative, then I is prime if and only if R/I is an integral domain. Similarly, we have

$$a + b\sqrt{-5} \equiv a - 2b \equiv 0, 1 \text{ or } 2 \mod I_3 \tag{13}$$

So we must have $R/I_3 \cong \mathbb{F}_3$, since our quotient ring can have at most 3 elements, and we get all three by appropriate choices of a, b. Hence again, since $\mathbb{F}_3$ is an integral domain, we have that I_3 must be a prime ideal. And I_3' is a prime ideal by the same reasoning, since the only thing that changes is that we have $a + 2b \equiv 0, 1 \text{ or } 2 \mod I_3'$, which again gives us $\mathbb{F}_3$ since $a + 2b \in \mathbb{Z}$. $\square$

(c) *Show that the factorizations in (a) imply the equality of the ideals* $(6) = (2)(3)$, *and* $(6) = (1 + \sqrt{-5})(1 - \sqrt{-5}) = (\alpha)(\overline{\alpha})$.

Proof. By multiplication of principle ideals, we know

$$(6) = (2)(3) = (\alpha)(\overline{\alpha}). \tag{14}$$

Also, note

$$I_3 I_3' = (3, 2 + \sqrt{-5})(3, 2 - \sqrt{-5}) = (9, 6 - 3\sqrt{-5}, 6 + 3\sqrt{-5}). \tag{15}$$

So $I_3 I_3' \subset (3)$ since 3 divides all the above generators. Also

$$3 = 9 + 6 - 3\sqrt{-5} + 6 + 3\sqrt{-5}, \tag{16}$$

so $(3) \subset I_3 I_3'$, and so $(3) = I_3 I_3'$. And so, using the results of the previous exercise, we have

$$(6) = (2)(3) = (I_2^2)(I_3 I_3') = (\alpha)(\overline{\alpha}) = (I_2 I_3)(I_2 I_3'), \tag{17}$$

and thus the factorization of the ideals is unique. $\square$