Math 1530: Homework 9

Milan Capoor

5 December 2023

7.1

Let R be an integral domain, and let $a, b \in R$. Prove that the following are equivalent:

(a) $a \mid b$ and $b \mid a$.

(b) There is a unit $u \in R^*$ satisfying $a = bu$.

(c) There is an equality of principal ideals $aR = bR$

By Definition 7.3, if $a \mid b$ then $bR \subseteq aR$. Similarly, if $b \mid a$ then $aR \subseteq bR$. Thus, $aR = bR$. So $(a) \implies (c)$.

Now suppose $aR = bR$. Then $a \in bR \implies a = bu \quad (u \in R)$ and $b \in aR \implies b = ac \quad (c \in R)$. Thus,

$$a = bu = (ac)u \implies cu = 1$$

Which means that u is a unit satisfying $a = bu$ and $(c) \implies (b)$

Finally, suppose we have a unit $u \in R^*$ with $a = bu$. Clearly, $b \mid a$. But by definition, there exists some $v \in R^*$ such that $uv = 1$. And so we can write

$$a = bu \implies a \cdot 1 = bu \cdot 1 \implies auv = bu \implies av = b \implies a \mid b$$

because R is an integral domain. Thus, $(b) \implies (a)$ and we have a loop of equivalences

$$(a) \to (c) \to (b) \to (a)$$

so we are done. ■

7.4

Let R be a Euclidean domain with size function σ, and let $a \in R$ be a non-zero element of R. Prove that

$$a \in R^* \iff \sigma(a) = \sigma(1)$$

If $a \in R^*$, then a is a unit. Thus, there exists some nonzero $b \in R$ such that $ab = 1$. By Proposition 7.15

$$\sigma(b) = \sigma(ab) = \sigma(1)$$

Further, by the properties of a size function,

$$\sigma(a) \leq \sigma(ab) = \sigma(1)$$

Now consider the ideal $I = (1) = R$. By Corollary 7.11, $\sigma(1) \leq \sigma(r)$ for every non-zero $r \in I = R$. Thus,

$$\sigma(a) \leq \sigma(1) \leq \sigma(a) \implies \sigma(a) = \sigma(1) \quad \square$$

Now for the other direction, suppose $\sigma(a) = \sigma(1)$. Then, since $a \neq 0$, we can write

$$1 = aq + r$$

with $\sigma(r) < \sigma(a)$.

But

$$\sigma(a) = 1 \implies \sigma(r) = 0 \implies 1 = aq$$

so a is a unit. ■

7.6

For a complex number $z = x + yi \in \mathbb{C}$, let $\sigma(z)$ be the square of its norm,

$$\sigma(z) = \sigma(x + yi) = x^2 + y^2$$

(a) Prove that $\sigma(z) = 0$ if and only if $z = 0$.

If $z = 0$, then $\sigma(z) = 0^2 + 0^2 = 0$.

Now suppose $\sigma(z) = 0$. Then $x^2 + y^2 = 0$. But $x^2, y^2 \geq 0$ so $x^2 + y^2 \geq 0$. So the only way for $\sigma(z)$ to be 0 is if $x^2 = y^2 = 0$. Thus, $z = 0$. ■

(b) Prove that $\sigma(z_1 z_2) = \sigma(z_1)\sigma(z_2)$.

Let $z_1 = a + bi$ and $z_2 = c + di$. Then

$$\begin{aligned}
\sigma(z_1 z_2) &= \sigma((a + bi)(c + di)) \\
&= \sigma((ac - bd) + (ad + bc)i) \\
&= (ac - bd)^2 + (ad + bc)^2 \\
&= a^2c^2 - 2abcd + b^2d^2 + a^2d^2 + 2adcb + b^2c^2 \\
&= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 \\
&= (a^2 + b^2)(c^2 + d^2) \\
&= \sigma(z_1)\sigma(z_2) \quad ■
\end{aligned}$$

(c) Is $\sigma(z_1 + z_2) = \sigma(z_1) + \sigma(z_2)$? If not, give a counterexample. Can you find an inequality relating these three quantities?

Again let $z_1 = a + bi$ and $z_2 = c + di$. Then

$$\begin{aligned}
\sigma(z_1 + z_2) &= \sigma((a + bi) + (c + di)) \\
&= \sigma((a + c) + (b + d)i) \\
&= (a + c)^2 + (b + d)^2 \\
&= a^2 + 2ac + c^2 + b^2 + 2bd + d^2 \\
&= (a^2 + b^2) + (c^2 + d^2) + 2(ac + bd) \\
&= \sigma(z_1) + \sigma(z_2) + 2(ac + bd)
\end{aligned}$$

So $\sigma(z_1 + z_2) = \sigma(z_1) + \sigma(z_2) + 2(ac + bd)$. Thus, $\sigma(z_1 + z_2) = \sigma(z_1) + \sigma(z_2)$ if and only if $ac + bd = 0$.

For example, let $z_1 = 2 + i$ and $z_2 = 1 + i$. Then

$$\begin{aligned} \sigma(z_1 + z_2) &= \sigma(3 + 2i) = 9 + 4 = 13 \\ \sigma(z_1) + \sigma(z_2) &= \sigma(2 + i) + \sigma(1 + i) = 5 + 2 = 7 \end{aligned}$$

so $\sigma(z_1) + \sigma(z_2) \leq \sigma(z_1 + z_2)$.

However, for $z_1 = 1 + i$ and $z_2 = -1 + i$, we have

$$\sigma(z_1 + z_2) = 4 = \sigma(z_1) + \sigma(z_2) = 4$$

so $\sigma(z_1 + z_2) = \sigma(z_1) + \sigma(z_2)$.

And finally, with $z_1 = 2 + i$ and $z_2 = -2 - i$, we have

$$\begin{aligned} \sigma(z_1 + z_2) &= 0 \\ \sigma(z_1) + \sigma(z_2) &= 5 + 5 = 10 \end{aligned}$$

so $\sigma(z_1 + z_2) \leq \sigma(z_1) + \sigma(z_2)$.

7.8

For each of the following rings R and elements α, determine whether α is irreducible in R. Justify your answer by either factoring α, or proving that it is irreducible. (Hint. For (a) and (b), it might be helpful to use the size function for $\mathbb{Z}[i]$.)

(a) $R = \mathbb{Z}[i]$, $\alpha = 2 + 3i$

First note that $\sigma(2 + 3i) = 2^2 + 3^2 = 13$. Let $\alpha = \zeta_1\zeta_2$. By Exercise 7.6, $\sigma(\zeta_1\zeta_1) = \sigma(\zeta_1)\sigma(\zeta_2)$ so

$$\sigma(\alpha) = \sigma(\zeta_1)\sigma(\zeta_2) = 13$$

But this means that $\sigma(\zeta_1) = 1$ and $\sigma(\zeta_2) = 13$ or vice versa. However, from exercise 7.4, we know that $\sigma(\zeta) = 1$ if and only if ζ is a unit. So α has a unit factor and is thus irreducible. ■

(b) $R = \mathbb{Z}[i]$, $\alpha = 4 + 3i$

$$\alpha = (1 + 2i)(2 - i)$$

(c) $R = \mathbb{F}_2[x]$, $\alpha = x^5 + x + 1$

$$\alpha = (x^2 + x + 1)(x^3 - x^2 + 1)$$

(d) $R = \mathbb{F}_2[x]$, $\alpha = x^5 + x^2 + 1$

From example 7.13, R is a Euclidean Domain so it is a PID. Consider the principal ideal $I = \alpha R$.

Consider two elements $a, b \in R$. Then $(a + I)(b + I) = ab + I$. Suppose $ab = 0$. But since

$$ab = \left(\sum_{i=1}^{n} a_i x^i\right)\left(\sum_{j=1}^{m} b_i x^j\right)$$

and $a_i, b_i \in \mathbb{F}_2$, every coefficient will be 0 or 1. Chiefly, this means that there will be no negative coefficients so the only way for the product to be zero is if one of the factors is 0. Hence, $\mathbb{F}_2[x]/\alpha F_2[x]$ is an integral domain. Then by Theorem 3.43, αR is prime so by Theorem 7.16, α is irreducible. ■

7.12

Let $R = \mathbb{Z}[\sqrt{3}]$ be the ring that we studied in Example 7.21.

(a) Prove that ±1 are the only units in R

Assume $a + b\sqrt{-3}$ is a unit in R. Then there exists some $c + d\sqrt{-3}$ such that

$$(a + b\sqrt{-3})(c + d\sqrt{-3}) = 1 \implies \begin{cases} ac - 3bd = 1 \\ ad + bc = 0 \end{cases}$$

We can solve this system of equations via

$$\begin{pmatrix} a & -3b \\ b & a \end{pmatrix} \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \implies \begin{pmatrix} c \\ d \end{pmatrix} = \frac{1}{a^2 + 3b^2} \begin{pmatrix} a \\ -b \end{pmatrix}$$

so

$$(a + b\sqrt{-3})(\frac{a}{a^2 + 3b^2} - \frac{b}{a^2 + 3b^2}\sqrt{-3}) = 1$$

$|a| = |a^2 + 3b^2|$ only in the cases $a, b = 0$ and $a = \pm 1, b = 0$. In the first case we have $0 = 1$ which is false and in the second, we get $1 = 1$ which is true. In any other case, the quantity $\frac{a}{a^2+3b^2} \notin \mathbb{Z}$ so the only units in R are ± 1. ■

(b) Prove that $1 + \sqrt{-3}$ and $1 - \sqrt{-3}$ are irreducible elements of R. (Hint. After you prove that $1 + \sqrt{-3}$ is irreducible, you can use Exercise 3.5(b) to prove that $1 - \sqrt{-3}$ is also irreducible.)

By part (a), they are not units.

Now we want to show that $1 + \sqrt{-3}$ has a unit factor. Consider

$$1 + \sqrt{-3} = (a + b\sqrt{-3})(c + d\sqrt{-3})$$

Expanding,

$$1 + \sqrt{-3} = (ac - 3bd) + (ad + bc)\sqrt{-3} \implies \begin{cases} ac - 3bd = 1 \\ ad + bc = 1 \end{cases}$$

solving for c and d gives

$$\begin{pmatrix} a & -3b \\ b & a \end{pmatrix} \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \implies \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} \frac{a+3b}{a^2+3b^2} \\ \frac{a-b}{a^2+3b^2} \end{pmatrix}$$

We want both of these to be solvable in the integers so

$$a - b = \lambda(a^2 + 3b^2) \quad \lambda \in \mathbb{Z} \implies \left|a^2 + 3b^2\right| \leq |a - b|$$

This is clearly true at $a, b = 0$ and $a = \pm 1, b = 0$ but $0 \neq 1 + \sqrt{-3}$ and

$$(1 + 0\sqrt{-3})(\frac{1 + 3(0)}{1 + 0}) = (1)(1) \neq 1 + \sqrt{-3}$$

In any case where $b > a$, the LHS is greater than the RHS. So we must have $b \leq a$. But at $a = 2, b = 1$, the LHS is already too large. Thus, there are no solutions in the integers and $1 + \sqrt{-3}$ is irreducible.

From exercise 3.5, we have a homomorphism $\phi(a + b\sqrt{-3}) = a - b\sqrt{-3}$. Suppose $1 - \sqrt{-3}$ is reducible. Then there exists some $a + b\sqrt{-3}$ such that

$$1 - \sqrt{-3} = (a + b\sqrt{-3})(c + d\sqrt{-3})$$

but since ϕ is a homomorphism from $\mathbb{Z}[\sqrt{-3}] \to \mathbb{Z}[\sqrt{-3}]$,

$$1 - \sqrt{-3} = (a + b\sqrt{-3})(c + d\sqrt{-3}) \implies \phi^{-1}(1 - \sqrt{-3}) = 1 + \sqrt{-3} = \phi^{-1}(a + b\sqrt{-3})\phi^{-1}(c + d\sqrt{-3})$$

But we just showed that $1 + \sqrt{-3}$ is irreducible so this is a contradiction. Thus, $1 - \sqrt{-3}$ is irreducible. ■

(c) Prove that 2 is an irreducible element of R. (We already proved this in the text, but try doing it yourself without looking back.)

By part (a), 2 is not a unit.

Does it factor into units? Consider,

$$2 = (a + b\sqrt{-3})(c + d\sqrt{-3}) = (a - b\sqrt{-3})(c - d\sqrt{-3})$$

Multiplying,

$$4 = (a + b\sqrt{-3})(c + d\sqrt{-3})(a - b\sqrt{-3})(c - d\sqrt{-3}) = (a^2 + 3b^2)(c^2 + 3d^2)$$

with $a, b, c, d \in \mathbb{Z}$.

We know the only integer factorizations are $4 = 2 \cdot 2 = 4 \cdot 1$.

Checking the first case,

$$\begin{cases} a^2 + 3b^2 = 2 \\ c^2 + 3d^2 = 2 \end{cases}$$

we find no solutions in the integers because if $b > 1$, then the LHS is greater than two and $a = \sqrt{2} \notin \mathbb{Z}$. Similar argument gives no solutions to the second case.

Thus, we try

$$\begin{cases} a^2 + 3b^2 = 4 \\ c^2 + 3d^2 = 1 \end{cases}$$

(or vice versa). The second line gives $c = \pm 1$ and $d = 0$ (or $a = \pm 1$ and $b = 0$). But then one of the factors of two is a unit, so it is irreducible. ■

(d) Use (a), (b), (c) and the formula

$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$$

to deduce that R is not a UFD.

From (a), (b), and (c), we have that 2, $1 + \sqrt{-3}$, $1 - \sqrt{-3}$ are irreducible elements of R. The formula shows that 4 has two distinct factorizations into irreducibles. Thus, R is not a UFD. ■