Math 1530: Homework 3

Milan Capoor

3 October 2023

3.5

We have already seen the ring of Gaussian integers $\mathbb{Z}[i]$. More generally, for any integer D that is not the square of an integer, we can form a ring

$$\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} : a, b \in \mathbb{Z}\}$$

If $D > 0$, then $\mathbb{Z}[\sqrt{D}]$ is a subring of $\mathbb{R}$, while if $D < 0$, then in any case it is a subring of $\mathbb{C}$

(a) Let $\alpha = 2 + 3\sqrt{5}$ and $\beta = 1 - 2\sqrt{5}$ be elements of $\mathbb{Z}[\sqrt{5}]$. Compute the quantities

$$\alpha + \beta, \quad \alpha \cdot \beta, \quad \alpha^2$$

$$\begin{aligned}
\alpha + \beta &= (2 + 3\sqrt{5}) + (1 - 2\sqrt{5}) &&= \boxed{3 + \sqrt{5}} \\
\alpha * \beta &= (2 + 3\sqrt{5})(1 - 2\sqrt{5}) = 2 - 4\sqrt{5} + 3\sqrt{5} - 6(5) &&= \boxed{-28 - \sqrt{5}} \\
\alpha^2 &= (2 + 3\sqrt{5})(2 + 3\sqrt{5}) = 4 + 6\sqrt{5} + 6\sqrt{5} + 9(5) &&= \boxed{49 + 12\sqrt{5}}
\end{aligned}$$

(b) Prove that the map

$$\phi : \mathbb{Z}[\sqrt{D}] \to \mathbb{Z}[\sqrt{D}], \quad \phi(a + b\sqrt{D}) = a - b\sqrt{D}$$

is a ring homomorphism. (For notational convenience, if $\alpha = a + b\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$, then people often write $\overline{\alpha} = a - b\sqrt{D}$, similar to the notation for complex conjugation.)

ϕ is a ring homomorphism if it satisfies the following three properties:

(a) $\phi(1) = 1$

$$\phi(1 + 0\sqrt{D}) = 1 - 0\sqrt{D} = 1 \quad \checkmark$$

(b) $\phi(a + b) = \phi(a) + \phi(b)$

$$\begin{aligned}
\phi([a_1 + a_2\sqrt{D}] + [b_1 + b_2\sqrt{D}]) &= \phi((a_1 + b_1) + (a_2 + b_2)\sqrt{D}) \\
&= (a_1 + b_1) - (a_2 + b_2)\sqrt{D} \\
&= a_1 + b_1 - a_2\sqrt{D} - b_2\sqrt{D} \\
&= [a_1 - a_2\sqrt{D}] + [b_2 - b_2\sqrt{D}] \\
&= \phi(a_1 + a_2\sqrt{D}) + \phi(b_1 + b_2\sqrt{D}) \quad \checkmark
\end{aligned}$$

(c) $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$

$$\begin{aligned}
\phi([a_1 + a_2\sqrt{D}] \cdot [b_1 + b_2\sqrt{D}]) &= \phi(a_1b_1 + a_1b_2\sqrt{D} + b_1a_2\sqrt{D} + a_2b_2D) \\
&= \phi([a_1b_1 + a_2b_2D] + [a_1b_2 + b_1a_2]\sqrt{D}) \\
&= [a_1b_1 + a_2b_2D] - [a_1b_2 + b_1a_2]\sqrt{D} \\
&= a_1b_1 + a_2b_2D - a_1b_2\sqrt{D} - b_1a_2\sqrt{D} \\
&= a_1b_1 - a_1b_2\sqrt{D} - b_1a_2\sqrt{D} + (a_2\sqrt{D})(b_2\sqrt{D}) \\
&= (a_1 - a_2\sqrt{D})(b_1 - b_2\sqrt{D}) \\
&= \phi(a_1 + a_2\sqrt{D}) \cdot \phi(b_1 + b_2\sqrt{D}) \quad \checkmark
\end{aligned}$$

(c) With notation as in (b), prove that

$$\alpha \cdot \overline{\alpha} \in \mathbb{Z} \quad \forall \alpha \in \mathbb{Z}[\sqrt{D}]$$

Let $\alpha = a + b\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$. Then

$$\begin{aligned}
\alpha \cdot \overline{\alpha} &= (a + b\sqrt{D})(a - b\sqrt{D}) \\
&= a^2 - b^2D
\end{aligned}$$

But we know that $a, b, D \in \mathbb{Z}$ so the quantity $a^2 - b^2D$ is in $\mathbb{Z}$. Thus, $\alpha\overline{\alpha} \in \mathbb{Z}$. ■

3.10

Prove that the map

$$\mathbb{C} \to M_2(\mathbb{R}), \quad x + yi \mapsto \begin{pmatrix} x & y \\ -y & x \end{pmatrix}$$

as discussed in Example 3.8, is an injective ring homomorphism

First, we verify that the map ϕ is a homomorphism:

1. $\phi(1) = 1$

   $$\phi(1 + 0i) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

   which is the multiplicative identity in $M_2(\mathbb{R})$ ✓

2. $\phi(a + b) = \phi(a) + \phi(b)$

   $$\begin{aligned} \phi([a_1 + a_2 i] + [b_1 + b_2 i]) &= \phi([a_1 + b_1] + [a_2 + b_2]i) \\ &= \begin{pmatrix} a_1 + b_1 & a_2 + b_2 \\ -a_2 - b_2 & a_1 + b_1 \end{pmatrix} \\ &= \begin{pmatrix} a_1 & a_2 \\ -a_2 & a_1 \end{pmatrix} + \begin{pmatrix} b_1 & b_2 \\ -b_2 & b_1 \end{pmatrix} \\ &= \phi(a_1 + a_2 i) + \phi(b_1 + b_2 i) \quad \checkmark \end{aligned}$$

3. $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$

   $$\begin{aligned} \phi([a_1 + a_2 i] \cdot [b_1 + b_2 i]) &= \phi([a_1 b_1 - a_2 b_2] + [a_1 b_2 + a_2 b_1]i) \\ &= \begin{pmatrix} a_1 b_1 - a_2 b_2 & a_1 b_2 + a_2 b_1 \\ -a_1 b_2 - a_2 b_1 & a_1 b_1 - a_2 b_2 \end{pmatrix} \\ &= \begin{pmatrix} a_1 & a_2 \\ -a_2 & a_1 \end{pmatrix} \begin{pmatrix} b_1 & b_2 \\ -b_2 & b_1 \end{pmatrix} \\ &= \phi(a_1 + a_2 i) \cdot \phi(b_1 + b_2 i) \quad \checkmark \end{aligned}$$

   So the mapping is a homomorphism.

   Now we need to show it is injective which amounts to showing that $\ker \phi = \{0\}$. Or, $\phi(a) = 0$ only for $a = 0$.

   First we check that $\phi(0) = 0$:

   $$\phi(0) = \phi(0 + 0i) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad \checkmark$$

So now all that remains is to show that $\phi(a) \neq 0$ for $a \neq 0$. This is easy as

$$\phi(a) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$$

with $a \in \mathbb{R}$ and $\mathbb{R}$ is a field so it is an integral domain. Thus there are no values $b \in \mathbb{R} - \{0\}$ for which $ab = 0$. Similarly, $a + b = 0$ only when $b = -a$.

Thus $\ker \phi = \{0\}$ and ϕ is an injective homomorphism. ■

3.20

Prove that each of the following rings is not a field:

(a) $\mathbb{Z}[i]$

Let $a = 2 + 0i = 2$. However, 2 does not have a multiplicative inverse in $\mathbb{Z}$ so we have found an element $a \in R$ with $a \neq 0$ that does not have a $b \in R$ with $ab = 1$. Thus, by definition, $\mathbb{Z}[i]$ is not a field. ■

(b) $\mathbb{R}[x]$

$\mathbb{R}[x]$ is the ring of polynomials $\left\{\sum_{i=0}^{d} a_i x^i : a_i \in \mathbb{R}, 0 \leq d\right\}$. Thus, exponents of negative degree are not in $\mathbb{R}[x]$. So we can identify the polynomial $x \in \mathbb{R}[x]$ which has no multiplicative inverse. Therefore, $\mathbb{R}[x]$ is not a field. ■

(c) $\mathbb{H}$

$\mathbb{H}$ cannot be a field because it is non-commutative:

$$j \cdot i = -i \cdot j, \quad k \cdot i = -i \cdot k, \quad k \cdot j = -j \cdot k \quad ■$$

(d) $M_n(\mathbb{R})$ if $n \geq 2$

$M_n(\mathbb{R})$ is not a commutative ring so it cannot be a field:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{pmatrix}$$
$$\begin{pmatrix} e & f \\ g & h \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ae + cf & be + df \\ ag + ch & bg + dh \end{pmatrix} \quad ■$$

3.29

(a) *Let R be a commutative ring, and suppose that its unit group R^* is finite, say $n = \#R^*$. Prove that every element $a \in R^*$ satisfies*

$$a^n = 1$$

Hint: Use Lagrange's Theorem, more specifically Corollary 2.50

By the Corollary of Lagrange's theorem, the order of any element $a \in R^*$ divides the order of the group, n. So, for some k,

$$n = k \cdot o(a)$$

Now consider a^n:

$$a^n = a^{k \cdot o(a)} = (a^{o(a)})^k = 1^k = 1$$

Thus, $a^n = 1$. ■

(b) *Let p be a prime, and let $a \in \mathbb{Z}$ be an integer with $p \nmid a$ Use (a) to prove:*

Fermat's Little Theorem: $a^{p-1} \equiv 1 \bmod p$

(Hint. Consider the unit group of $\mathbb{Z}/p\mathbb{Z}$.)

Consider the group $(\mathbb{Z}/p\mathbb{Z})^*$. Because p is prime, the order of the group is $p - 1$ (because the group is simply $\{1, 2, \ldots, p\}$) By (a), we have an element in $\alpha \in (\mathbb{Z}/p\mathbb{Z})^*$ for which

$$\alpha^{p-1} = 1$$

But by the definition of $(\mathbb{Z}/p\mathbb{Z})^*$,

$$\alpha \in \{a \bmod p : \gcd(a, p) = 1\}$$

And as p is prime, a can be any number which is not a multiple of p. So

$$(a \bmod p)^{p-1} = 1 \implies a^{p-1} \equiv 1 \bmod p \quad ■$$

3.30

(a) *Compute the unit group* $(\mathbb{Z}/p\mathbb{Z})^*$ *for each of the primes* $p = 7, 11, 13$. *Which ones are cyclic?*

By Proposition 3.20,

$$(\mathbb{Z}/p\mathbb{Z})^* = \{a \bmod p : \gcd(a, p) = 1\}$$

(a) $p = 7$

First we note that $\gcd(a, 7) = 1$ for all $1 \leq a < 7$. So

$$(\mathbb{Z}/7\mathbb{Z})^* = \{1, 2, 3, 4, 5, 6\}$$

It is cyclic because

$$\begin{aligned}
3^2 &\equiv 2 \bmod 7 \in (\mathbb{Z}/7\mathbb{Z})^* \\
3^3 &\equiv 6 \bmod 7 \in (\mathbb{Z}/7\mathbb{Z})^* \\
3^4 &\equiv 4 \bmod 7 \in (\mathbb{Z}/7\mathbb{Z})^* \\
3^5 &\equiv 5 \bmod 7 \in (\mathbb{Z}/7\mathbb{Z})^* \\
3^6 &\equiv 1 \bmod 7 \in (\mathbb{Z}/7\mathbb{Z})^* \\
3^7 &\equiv 3 \bmod 7 \in (\mathbb{Z}/7\mathbb{Z})^*
\end{aligned}$$

(b) $p = 11$

Again, because p is prime,

$$(\mathbb{Z}/11\mathbb{Z})^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$$

and it is cyclic:

$$\begin{aligned}
2^1 &\equiv 2 \bmod 11 \in (\mathbb{Z}/11\mathbb{Z})^* \\
2^2 &\equiv 4 \bmod 11 \in (\mathbb{Z}/11\mathbb{Z})^* \\
2^3 &\equiv 8 \bmod 11 \in (\mathbb{Z}/11\mathbb{Z})^* \\
2^4 &\equiv 5 \bmod 11 \in (\mathbb{Z}/11\mathbb{Z})^* \\
2^5 &\equiv 10 \bmod 11 \in (\mathbb{Z}/11\mathbb{Z})^* \\
2^6 &\equiv 9 \bmod 11 \in (\mathbb{Z}/11\mathbb{Z})^* \\
2^11 &\equiv 7 \bmod 11 \in (\mathbb{Z}/11\mathbb{Z})^* \\
2^8 &\equiv 3 \bmod 11 \in (\mathbb{Z}/11\mathbb{Z})^* \\
2^9 &\equiv 6 \bmod 11 \in (\mathbb{Z}/11\mathbb{Z})^* \\
2^{10} &\equiv 1 \bmod 11 \in (\mathbb{Z}/11\mathbb{Z})^*
\end{aligned}$$

(c) $p = 13$

$$(\mathbb{Z}/13\mathbb{Z})^* = \{n : 1 \leq n < 13,\ n \in \mathbb{Z}\}$$

With generator 2:

$$\begin{aligned}
2^1 &\equiv 2 \bmod 13 \in (\mathbb{Z}/13\mathbb{Z})^* \\
2^2 &\equiv 4 \bmod 13 \in (\mathbb{Z}/13\mathbb{Z})^* \\
2^3 &\equiv 8 \bmod 13 \in (\mathbb{Z}/13\mathbb{Z})^* \\
2^4 &\equiv 3 \bmod 13 \in (\mathbb{Z}/13\mathbb{Z})^* \\
2^5 &\equiv 6 \bmod 13 \in (\mathbb{Z}/13\mathbb{Z})^* \\
2^6 &\equiv 12 \bmod 13 \in (\mathbb{Z}/13\mathbb{Z})^* \\
2^7 &\equiv 11 \bmod 13 \in (\mathbb{Z}/13\mathbb{Z})^* \\
2^8 &\equiv 9 \bmod 13 \in (\mathbb{Z}/13\mathbb{Z})^* \\
2^9 &\equiv 5 \bmod 13 \in (\mathbb{Z}/13\mathbb{Z})^* \\
2^{10} &\equiv 10 \bmod 13 \in (\mathbb{Z}/13\mathbb{Z})^* \\
2^{11} &\equiv 7 \bmod 13 \in (\mathbb{Z}/13\mathbb{Z})^* \\
2^{12} &\equiv 1 \bmod 13 \in (\mathbb{Z}/13\mathbb{Z})^*
\end{aligned}$$

(b) *Compute the unit group* $(\mathbb{Z}/m\mathbb{Z})^*$ *for each of the composite numbers* $m = 8$, *9, 15. Which ones are cyclic?*

(a) $m = 8$

$$(\mathbb{Z}/8)^* = \{1, 3, 5, 7\}$$

Is not cyclic because there is not a generator.

(b) $m = 9$

$$(\mathbb{Z}/9\mathbb{Z})^* = \{1, 2, 4, 5, 7, 8\}$$

Is cyclic because

$$\begin{aligned}
2^1 &\equiv 2 \bmod 9 \in (\mathbb{Z}/9\mathbb{Z})^* \\
2^2 &\equiv 4 \bmod 9 \in (\mathbb{Z}/9\mathbb{Z})^* \\
2^3 &\equiv 8 \bmod 9 \in (\mathbb{Z}/9\mathbb{Z})^* \\
2^4 &\equiv 7 \bmod 9 \in (\mathbb{Z}/9\mathbb{Z})^* \\
2^5 &\equiv 5 \bmod 9 \in (\mathbb{Z}/9\mathbb{Z})^* \\
2^6 &\equiv 1 \bmod 9 \in (\mathbb{Z}/9\mathbb{Z})^* \\
5^1 &\equiv 5 \bmod 9 \in (\mathbb{Z}/9\mathbb{Z})^* \\
5^2 &\equiv 7 \bmod 9 \in (\mathbb{Z}/9\mathbb{Z})^* \\
5^3 &\equiv 8 \bmod 9 \in (\mathbb{Z}/9\mathbb{Z})^* \\
5^4 &\equiv 4 \bmod 9 \in (\mathbb{Z}/9\mathbb{Z})^* \\
5^5 &\equiv 2 \bmod 9 \in (\mathbb{Z}/9\mathbb{Z})^* \\
5^6 &\equiv 1 \bmod 9 \in (\mathbb{Z}/9\mathbb{Z})^*
\end{aligned}$$

(c) $m = 15$

$$(\mathbb{Z}/15\mathbb{Z})^* = \{1, 2, 4, 7, 8, 9, 11, 13, 14\}$$

Is, once again, not cyclic.

3.32

Prove that the product ring $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ *is isomorphic to the ring* $\mathbb{Z}/6\mathbb{Z}$ *by writing down an explicit isomorphism* $\mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

$\phi(a \bmod 6) = (a \bmod 2, a \bmod 3)$ is an isomorphism from $\mathbb{Z}/6 \to \mathbb{Z}/2 \times \mathbb{Z}/3$ by Example 2.55 because $\gcd(3, 2) = 1$ and $3 \cdot 2 = 6$.

Therefore, the product ring $\mathbb{Z}/2 \times \mathbb{Z}/3$ is isomorphic to $\mathbb{Z}/6$. ■