THE CHINESE UNIVERSITY OF HONG KONG
Department of Mathematics
MATH 2070A Algebraic Structures 2019-20
Tutorial 7
Date: 4th November 2019

Problems:

1. Under the addition and multiplication as the operations in $\mathbb{C}$, determine whether the following set is a ring or a field: $A = \{a + b\sqrt{3} : a, b \in \mathbb{Z}\}$, $B = \{a + be^{2\pi i/3} : a, b \in \mathbb{Z}\}$, $C = \{a + b\sqrt{3} : a, b \in \mathbb{Q}\}$.

   Solution. Clearly A, B, and C are groups under $+$. For multiplication, it is well-defined in A, B and C. For B, note that

   $$(a+be^{2\pi i/3})(c+de^{2\pi i/3}) = ab+cde^{4\pi i/3}+(ac+bd)e^{2\pi i/3} = ab-cd+(ac+bd-cd)e^{2\pi i/3}$$

   since $e^{4\pi i/3} = -1 - e^{2\pi i/3}$. Next, by direct checking the multiplication in A, B and C are associative and satisfy the distributive law. The number 1 plays the role of unity in A, B and C. Note also that A, B and C are (commutative) rings.

   Clearly A is not a field because, for example, 2 does not have multiplicative inverse $(2(a + b\sqrt{3}) = 1 \Rightarrow a = 1/2 \notin \mathbb{Z})$. But A is an integral domain because

   $$(a+b\sqrt{3})(c+d\sqrt{3}) = 0 \Rightarrow (a-b\sqrt{3})(a+b\sqrt{3})(c+d\sqrt{3})(c-d\sqrt{3}) \Rightarrow a^2 = 3b^2 \text{ or } c^2 = 3d^2$$

   which says that $a = b = 0$ or $c = d = 0$.

   B is not a field as $4e^{2\pi i/3}$ has no multiplicative inverse. Suppose $4e^{2\pi i/3}$ has a multiplicative inverse, we then have

   $$4e^{2\pi i/3}(a+be^{2\pi i/3}) = 1 \Rightarrow 2e^{2\pi i/3}(2a+2be^{2\pi i/3}) = 1 \xRightarrow{e^{2\pi i/3}=-\frac{1}{2}+\frac{\sqrt{3}i}{2}} 2\left((2a-b)^2 + 3b^2\right) = 1$$

   which is absurd. But B is an integral domain because

   $$\begin{aligned} & (a + be^{2\pi i/3})(c + de^{2\pi i/3}) = 0 \\ \Rightarrow\ & (a - b/2 - b\sqrt{3}i/2)(a - b/2 + b\sqrt{3}i/2)(c - d/2 - d\sqrt{3}i/2)(c - d/2 + d\sqrt{3}i/2) = 0 \\ \Rightarrow\ & (2a - b)^2 + 3b^2 = 0 \text{ or } (2c - d)^2 + 3d^2 = 0 \end{aligned}$$

   which says that $a = b = 0$ or $c = d = 0$.

   Let $a + b\sqrt{3} \neq 0$. Then $a^2 - 3b^2 \neq 0$. The multiplicative inverse of $a + b\sqrt{3}$ is given by $\frac{a}{a^2-3b^2} - \frac{b}{a^2-3b^2}\sqrt{3}$. Thus C is a field.

   ◀

2. Find all the units in the indicated rings.

(a) $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$

(b) $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$

(c) $\mathbb{Q}[i] = \{a + bi : a, b \in \mathbb{Q}\}$

(d) $M(2, \mathbb{Z})$

(e) $\mathbb{Z}_{12}$

Solution. (a) If $(a+bi)(c+di) = 1$, then $(a^2+b^2)(c^2+d^2) = 1$ by taking the modulus. Since $a, b, c, d \in \mathbb{Z}$, we must have $a^2 + b^2 = 1$. This suggests that 1, -1, i, and $-i$ are the only units in $\mathbb{Z}[i]$.

(b) If $(a+b\sqrt{-5})(c+d\sqrt{-5}) = 1$, then $(a^2+5b^2)(c^2+5d^2) = 1$ by taking the modulus. Since $a, b, c, d \in \mathbb{Z}$, we must have $a^2 + 5b^2 = 1$. This suggests that 1 and -1 are the only units in $\mathbb{Z}[\sqrt{-5}]$.

(c) For non-zero rational numbers a, b, $a + bi$ has the inverse $\frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i$. So every non-zero element in $\mathbb{Q}[i]$ is a unit.

(d) The inverse of a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is given by $\frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. So the inverse exists and is an integer matrix if and only if the determinant is ± 1. It follows that all such matrices make up the units of $M(2, \mathbb{Z})$. In other words, the units in $M(2, \mathbb{Z})$ form the set $\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M(2, \mathbb{Z}) : ad - bc = \pm 1\right\}$.

(e) Suppose that $xy \equiv 1 \pmod{12}$. $12|(xy - 1)$ implies that x and y are both odd and both x and y are not divisible by 3. By direct checking, one gets $\{1, 5, 7, 11\}$ are the only units in $\mathbb{Z}_{12}$. In fact $1^2 \equiv 5^2 \equiv 7^2 \equiv 11^2 \equiv 1 \pmod{12}$.

◀

3. Show that the ring $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ has infinitely many units.

Solution. Consider $x = 1 + \sqrt{2}$. This x has the inverse $-1 + \sqrt{2}$, so it is a unit. We immediately check that all x^n where n is a positive integer are different units in $\mathbb{Z}[\sqrt{2}]$ (as $\{x^n\}$ is strictly increasing).

◀

4. Let R be a ring with $1 \neq 0$. Let $a, b \in R$ such that $ab = 1$.

(a) Prove that if a is not a zero divisor, then $ba = 1$.

(b) Prove that if b is not a zero divisor, then $ba = 1$.

Solution. (a) Suppose a is not a zero divisor.

$$(ab-1)a = aba - a = a(ba-1) = 0$$

so $ba = 1$ as a is not a zero divisor.

(b) Suppose b is not a zero divisor.

$$b(ab-1) = bab - b = (ba-1)b = 0$$

so $ba = 1$ as b is not a zero divisor.

◀

5. Prove that every non-zero element in a finite ring is either a unit or a zero divisor.

Solution. Let $a \in R$ and consider the map on R given by $x \mapsto ax$. If this map is injective then it has to be surjective, because R is finite. Hence, $1 = ax$ for some $x \in R$ and a is a unit. If the map is not injective then there are $u, v \in R$, with $u \neq v$, such that $au = av$. But then $a(u-v) = 0$ and $u - v \neq 0$ and so a is a zero divisor. ◀

6. True or false: every non-zero element in a ring is either a unit or a zero divisor.

Solution. False. Consider $\mathbb{Z}$. Then 2 is neither a zero-divisor nor a unit. ◀

Optional Part

1. Let R be a ring and $a, b \in R$. Show that $1 - ab$ is a unit in R if and only if $1 - ba$ is a unit in R.

Solution. It suffices to show that if $1 - ab$ is a unit in R then $1 - ba$ is a unit in R. Let u be the inverse for $1 - ab$. Then $1 + bua$ is the inverse of $1 - ba$. Indeed

$$(1-ba)(1+bua) = 1 - ba + bua - babua = 1 - ba + b(1-ab)ua = 1 - ba + ba = 1.$$

◀

2. Let R be a ring and assume that whenever $ab = ca$ for some elements $a, b, c \in R$, we have $b = c$. Then prove that R is a commutative ring.

Solution. Let x, y be arbitrary elements in R. We want to show that $xy = yx$. Consider the identity $y(xy) = (yx)y$. This can be written as $ab = ca$ if we put $a = y, b = xy, c = yx$. It follows from the assumption that we have $b = c$. Equivalently, we have $xy = yx$. Thus R is a commutative ring. ◀