Math 3140 - Assignment 14

Due April 26, 2021

(1) Let c be an integer and let $\sqrt{c} \in \mathbb{C}$ such that $(\sqrt{c})^2 = c$. Show that

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

is a subring of the field $(\mathbb{C}, +, \cdot)$.

Is $\mathbb{Z}[\sqrt{c}]$ an integral domain? Is $\mathbb{Z}[\sqrt{c}]$ a subfield?

$\mathbb{Z}[i]$ is called the ring of *Gaussian integers*.

Solution. Let $a + b\sqrt{c}, d + e\sqrt{c} \in \mathbb{Z}[\sqrt{c}]$. Then

$$[a + b\sqrt{c}] + [d + e\sqrt{c}] = (a + d) + (b + e)\sqrt{c} \in \mathbb{Z}[\sqrt{c}]$$
$$-(a + b\sqrt{c}) = -a - b\sqrt{c} \in \mathbb{Z}[\sqrt{c}]$$

shows that $\mathbb{Z}[\sqrt{c}]$ is a subgroup of $(\mathbb{C}, +)$. Further

$$[a + b\sqrt{c}] \cdot [d + e\sqrt{c}] = ad + bec + (ae + bd))\sqrt{c} \in \mathbb{Z}[\sqrt{c}]$$

shows that $\mathbb{Z}[\sqrt{c}]$ is closed under multiplication, hence a subring of $(\mathbb{C}, +, \cdot)$.

As subring of an integral domain, $\mathbb{Z}[\sqrt{c}]$ has no zero divisors and is an integral domain itself.

Still $\mathbb{Z}[\sqrt{c}]$ is not a field since e.g. 2 has no multiplicative inverse. Note that subrings of fields need not be subfields. □

(2) Let R be a finite commutative ring with 1. Show that every $a \in R \setminus \{0\}$ is either a unit or a zero divisor.

Find an infinite R for which this is not true.

Hint: Consider whether $aR = R$ or not.

Solution. Let $a \in R \setminus \{0\}$. Note that $\varphi \colon R \to R, \ x \mapsto ax$, is a group homomorphism of $(R, +)$ by distributivity.

Case, φ is injective: By the finiteness of R this means that φ is bijective, hence $aR = R$. In particular there exists $b \in R$ such that $ab = 1$. Thus a is a unit.

Case, φ is not injective: Then $\ker \varphi \neq 0$ and there exists $b \in \ker \varphi \setminus \{0\}$ such that $ab = 0$. Thus a is a zero divisor.

Finiteness of R is necessary since e.g. in $\mathbb{Z}$ we see that 2 is neither a unit nor a zero divisor. □

(3) (a) Show that if an ideal I of a ring R contains a unit, then $I = R$.

(b) Conclude that the only ideals of a field F are 0 and F.

Solution. (a) Assume that $a \in I$ is a unit with inverse b. Then $1 = ba$ is in I. Further for every $r \in R$ we have $r = rba \in R$. So $R = I$.
(b) Let $I \neq 0$ be an ideal of a field F. Then I contains a non zero element, hence a unit. So $I = F$ by (a). □

(4) Let R be a commutative ring with 1, let $a_1, \ldots, a_n \in R$.
(a) Show that

$$(a_1, \ldots, a_n) := \{r_1 a_1 + \cdots + r_n a_n \ : \ r_1, \ldots, r_n \in R\}$$

is an ideal of R.
(b) Show that any ideal I of R that contains $a_1, \ldots, a_n$ also contains $(a_1, \ldots, a_n)$. Thus $(a_1, \ldots, a_n)$ is the smallest ideal containing $a_1, \ldots, a_n$.

Solution. (a) Clearly $(a_1, \ldots, a_n)$ is closed under $+$ and $-$, hence a subgroup of R. Let $r_1, \ldots, r_n \in R$ and $s \in R$. Then

$$s(r_1 a_1 + \cdots + r_n a_n) = sr_1 a_1 + \cdots + sr_n a_n \in (a_1, \ldots, a_n).$$

Hence $(a_1, \ldots, a_n)$ is also an ideal.
(b) If an ideal I of R contains $a_1, \ldots, a_n$, then it also contains $r_1 a_1, \ldots, r_n a_n$ and $r_1 a_1 + \cdots + r_n a_n$ by the ideal properties for all $r_1, \ldots, r_n \in R$. Hence $(a_1, \ldots, a_n) \subseteq I$. □

(5) Let I, J be ideals in a ring R. Show that their sum

$$I + J := \{i + j \ : \ i \in I, j \in J\}$$

is an ideal of R.

What is the sum of the ideals (12) and (18) in $\mathbb{Z}$?

Solution. $I + J$ is a subgroup: Let $i_1, i_2 \in I, j_1, j_2 \in J$. Then $(i_1 + j_1) + (i_2 + j_2) = (i_1 + i_2) + (j_1 + j_2) \in I + J$ using that $(R, +)$ is abelian. Further $-(i_1 + j_1) = -i_1 + (-j_1) \in I + J$.

From distributivity we get $R(I + J) = RI + RJ \subseteq I + J$. Similarly $(I + J)R = IR + JR \subseteq I + J$. Hence $I + J$ is an ideal.

In $\mathbb{Z}$ we have

$$(12) + (18) = \{12x + 18y \ : \ x, y \in \mathbb{Z}\} = 6\mathbb{Z} = (6)$$

More generally $(m) + (n) = (\gcd(m, n))$ by Bezout's identity.

(6) Show that the following pairs of rings are not isomorphic.
(a) $2\mathbb{Z}$ and $3\mathbb{Z}$
(b) $\mathbb{R} \times \mathbb{R}$ and $\mathbb{C}$
(c) $\mathbb{R}$ and $\mathbb{C}$

Solution. Find properties for which these rings are different to show that they are not isomorphic.
(a) Suppose $\varphi\colon 2\mathbb{Z} \to \mathbb{Z}$ is a ring isomorphism. Then φ is in particular an isomorphism between the cyclic groups $(2\mathbb{Z}, +)$ and $(3\mathbb{Z}, +)$. So φ maps generators to each other. Either $\varphi(2) = 3$ or $\varphi(2) = -3$.

Suppose $\varphi(2) = 3$. Then

$$\varphi(2+2) = 3+3 = 6 \quad \varphi(2\cdot 2) = 3\cdot 3 = 9$$

give a contradiction. Similar for $\varphi(2) = -3$. So there cannot be a ring isomorphism between $2\mathbb{Z}$ and $3\mathbb{Z}$.
(b) $\mathbb{R}\times\mathbb{R}$ has zero divisors $(1,0)\cdot(0,1) = (0,0)$ but $\mathbb{C}$ is a field. Hence they are not isomorphic.
(c) The multiplicative group of $\mathbb{C}$ has an element i of order 4. But the only elements of finite order in the multiplicative group of $\mathbb{R}$ are $1, -1$. Hence they are not isomorphic. □

(7) Show that $\mathbb{R}[x]/(f)$ for $f = x^2 + 1$ is isomorphic to the field of complex numbers $\mathbb{C}$.

Hint: Note that elements in the quotient ring are of the form $a + bx + (f)$. What are the sum and the product of two such elements?

Solution. Note that

$$[a + bx + (f)] + [c + dx + (f)] = (a + c) + (b + d)x + (f)$$

$$[a+bx+(f)]\cdot[c+dx+(f)] = ac+(ad+bc)x+bdx^2+(f) = ac-bd+(ad+bc)x+(f)$$

where the last equality follows from the fact that $1+x^2+(f) = 0+(f)$, that is $x^2 \equiv -1 \mod (f)$.

Now it is easy to see that

$$\mathbb{C} \to \mathbb{R}[x]/(f),\ a + bi \mapsto a + bx + (f),$$

is a unital ring isomorphism. □