

## Solutions to Homework #19

1. Saracino, Section 18, Problem 18.6:

Prove that the ring  $R = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$  has precisely two automorphisms.

**Proof.** Define  $f_1 : R \rightarrow R$  by  $f_1(a + b\sqrt{2}) = a + b\sqrt{2}$  and  $f_2 : R \rightarrow R$  by  $f_2(a + b\sqrt{2}) = a - b\sqrt{2}$ .

**Claim 1.** Both  $f_1$  and  $f_2$  are automorphisms.

**Proof of Claim 1.** This is clear for  $f_1$ , because it is the identity function, and hence  $f_1$  is bijective, and for any  $x, y \in R$ , we have  $f_1(x + y) = x + y = f_1(x) + f_1(y)$  and  $f_1(xy) = xy = f_1(x)f_1(y)$ .

As for  $f_2$ , observe first that  $f_2 \circ f_2$  is the identity function on  $R$ , and hence  $f_2$  is its own inverse. Being invertible,  $f_2$  is bijective. To finish the proof of the claim, it remains to show that  $f_2$  is a ring homomorphism.

Given  $x, y \in R$ , write  $x = a + b\sqrt{2}$  and  $y = c + d\sqrt{2}$ , with  $a, b \in \mathbb{Z}$ . Then

$$f_2(x + y) = f_2((a + c) + (b + d)\sqrt{2}) = (a + c) - (b + d)\sqrt{2} = (a - b\sqrt{2}) + (c - d\sqrt{2}) = f_2(x) + f_2(y),$$

and

$$f_2(xy) = f_2((ac + 2bd) + (ad + bc)\sqrt{2}) = (ac + 2bd) - (ad + bc)\sqrt{2} = (a - b\sqrt{2})(c - d\sqrt{2}) = f_2(x)f_2(y).$$

QED Claim 1

Moreover, since  $f_1(\sqrt{2}) = \sqrt{2} \neq -\sqrt{2} = f_2(\sqrt{2})$ , we have  $f_1 \neq f_2$ . Thus, we have found two automorphisms of  $R$ ; it suffices to show these are the only two.

Given an automorphism  $\varphi$  of  $R$ , define  $w = \varphi(\sqrt{2})$ .

**Claim 2.** For any  $a, b \in \mathbb{Z}$ , we have  $\varphi(a + b\sqrt{2}) = a + bw$ .

**Proof of Claim 2.** We have  $\varphi(1) = 1$  because  $\varphi$  is onto, by Theorem 18.2(i). For any  $a, b \in \mathbb{Z}$ , Theorem 18.1(ii) gives

$$\varphi(a) = \varphi(a \cdot 1) = a\varphi(1) = a \cdot 1 = a, \text{ and } \varphi(b\sqrt{2}) = b\varphi(\sqrt{2}) = bw.$$

Thus, because  $\varphi$  is a homomorphism, we have  $\varphi(a + b\sqrt{2}) = a + bw$ .

QED Claim 2

By Claim 2 with  $a = 2$  and  $b = 0$ , we have  $\varphi(2) = 2$ . Therefore, since  $\varphi$  is a homomorphism, we have

$$w^2 = \varphi(\sqrt{2})^2 = \varphi(\sqrt{2} \cdot \sqrt{2}) = \varphi(2) = 2.$$

Since  $R \subseteq \mathbb{R}$ , and the only real numbers whose square is 2 are  $\pm\sqrt{2}$ , we have  $w = \sqrt{2}$  or  $w = -\sqrt{2}$ .

If  $w = \sqrt{2}$ , then by Claim 2, we have  $\varphi(x) = x$  for all  $x \in R$ , and therefore  $\varphi = f_1$ . Otherwise, we have  $w = -\sqrt{2}$ , and hence for any  $a, b \in \mathbb{Z}$ , we have  $\varphi(a + b\sqrt{2}) = a - b\sqrt{2}$ , and therefore  $\varphi = f_2$ , as desired.

QED

2. Saracino, Section 18, Problem 18.15:

Let  $\varphi : R \rightarrow S$  be a (ring) homomorphism. Prove that  $\varphi$  is one-to-one if and only if  $\ker \varphi = \{0_R\}$ .

**Proof 1.**  $(\Rightarrow) (\subseteq)$ : Given  $x \in \ker \varphi$ , we have  $\varphi(x) = 0_S$ . However, we also have  $\varphi(0_R) = 0_S$ , because  $\varphi$  is a homomorphism. Therefore, because  $\varphi$  is one-to-one, we have  $x = 0_R$ , as desired.

$(\supseteq)$ : Since  $\varphi$  is a homomorphism, we have  $\varphi(0_R) = 0_S$ , so that  $0_R \in \ker \varphi$ , as desired. QED  $(\Rightarrow)$

$(\Leftarrow)$  Given  $x, y \in R$  with  $\varphi(x) = \varphi(y)$ , we have

$$\varphi(x - y) = \varphi(x) - \varphi(y) = 0_S,$$

and hence  $x - y \in \ker \varphi$ , and therefore  $x - y = 0_R$ . That is,  $x = y$ .

QED

**Proof 2.** Considering  $(R, +)$  and  $(S, +)$  as groups under addition, and  $\varphi$  as a group homomorphism, the ring definition of  $\ker \varphi$  coincides with our old group definition of  $\ker \varphi$ .

By Theorem 13.1 [the proof of which was a prior homework problem] applied to this group homomorphism, we have that  $\varphi$  is one-to-one if and only if  $\ker \varphi = \{0_R\}$ . QED

3. Saracino, Section 18, Problem 18.22(a):

Let  $\varphi : R \rightarrow S$  be a (ring) homomorphism, and let  $J$  be a prime ideal of  $S$ . If  $\varphi^{-1}(J) \neq R$ , prove that  $\varphi^{-1}(J)$  is a prime ideal of  $R$ .

**Proof. (Nonempty):** We have  $\varphi(0_R) = 0_S \in J$ , and hence  $0_R \in \varphi^{-1}(J)$ .

**(Closed):** Given  $x, y \in \varphi^{-1}(J)$ , we have  $\varphi(x), \varphi(y) \in J$ , and hence

$$\varphi(x - y) = \varphi(x) - \varphi(y) \in J,$$

so  $x - y \in \varphi^{-1}(J)$ .

**(Sticky):** Given  $x \in \varphi^{-1}(J)$  and  $r \in R$ , we have  $\varphi(x) \in J$ , and hence

$$\varphi(rx) = \varphi(r)\varphi(x) \in J \quad \text{and} \quad \varphi(xr) = \varphi(x)\varphi(r) \in J,$$

and so  $rx, xr \in \varphi^{-1}(J)$ .

**(Prime):** By hypothesis, we already know that  $\varphi^{-1}(J) \neq R$ .

Given  $a, b \in R$  with  $ab \in \varphi^{-1}(J)$ , we have  $\varphi(a)\varphi(b) = \varphi(ab) \in J$ , and hence either  $\varphi(a) \in J$  or  $\varphi(b) \in J$ , since  $J$  is prime. Thus, either  $a \in \varphi^{-1}(J)$  or  $b \in \varphi^{-1}(J)$ . QED

4. Saracino, Section 18, Problem 18.28:

In the proof of Theorem 18.10, we had an integral domain  $D$  and a set  $F$  called the field of fractions of  $D$ . Prove that the operations  $+$  and  $\cdot$  defined on  $F$  in that proof are well-defined.

**Proof.** Given  $a_1, b_1, a_2, b_2, c_1, c_2, d_1, d_2 \in D$  with  $b_1, b_2, d_1, d_2 \neq 0$  and  $\overline{(a_1, b_1)} = \overline{(a_2, b_2)}$  and  $\overline{(c_1, d_1)} = \overline{(c_2, d_2)}$ , we have  $a_1b_2 = a_2b_1$  and  $c_1d_2 = c_2d_1$ .

Therefore,

$$(b_1d_1)(a_2d_2 + b_2c_2) = (a_2b_1)(d_1d_2) + (b_1b_2)(c_2d_1) = (a_1b_2)(d_1d_2) + (b_1b_2)(c_1d_2) = (b_2d_2)(a_1d_1 + b_1c_1),$$

and hence

$$\overline{(a_1, b_1)} + \overline{(c_1, d_1)} = \overline{(a_1d_1 + b_1c_1, b_1d_1)} = \overline{(a_2d_2 + b_2c_2, b_2d_2)} = \overline{(a_2, b_2)} + \overline{(c_2, d_2)},$$

proving that  $+$  is well-defined. Similarly,

$$(b_1d_1)(a_2c_2) = (a_2b_1)(c_2d_1) = (a_1b_2)(c_1d_2) = (b_2d_2)(a_1c_1),$$

and hence

$$\overline{(a_1, b_1)} \cdot \overline{(c_1, d_1)} = \overline{(a_1c_1, b_1d_1)} = \overline{(a_2c_2, b_2d_2)} = \overline{(a_2, b_2)} \cdot \overline{(c_2, d_2)},$$

proving that  $\cdot$  is well-defined. QED

5. Saracino, Section 19, Problem 19.1:

Let  $f(X) = a_0 + a_1X + \cdots + a_rX^r \in \mathbb{Z}[X]$ . Suppose  $m/n \in \mathbb{Q}$ , with  $(m, n) = 1$ . If  $m/n$  is a root of  $f$ , prove that  $m|a_0$  and  $n|a_r$ .

**Proof.** We have  $0 = f(m/n) = a_0 + a_1mn^{-1} + a_2m^2n^{-2} + \cdots + a_rm^rn^{-r}$ . Multiplying by  $n^r$ , then,

$$a_0n^r + a_1mn^{r-1} + a_2m^2n^{r-2} + \cdots + a_rm^r = 0.$$

In particular,

$$a_0n^r = m(-a_1n^{r-1} - a_2mn^{r-2} - \cdots - a_rm^{r-1}),$$

and hence  $m|(a_0n^r)$ , since the expression in parenthesis is an integer. Since  $(m, n) = 1$ , repeated application of Theorem 4.3 shows that  $m|a_0$ , as desired.

Similarly, we also have

$$a_rm^r = n(-a_0n^{r-1} - a_1mn^{r-2} - \cdots - a_{r-1}m^{r-1}),$$

and hence  $n|(a_rm^r)$ . Again because  $(m, n) = 1$ , it follows that  $n|a_r$ . QED