

## Solutions to Problem Set 9.

1. Prove that for two ideals  $I_1 = \langle d_1 \rangle$  and  $I_2 = \langle d_2 \rangle$  in  $\mathbb{Z}$ , there is an inclusion  $I_1 \subseteq I_2$  iff  $d_2 | d_1$ .

**Solution.** If  $I_1 \subseteq I_2$ , then in particular,  $d_1 \in I_2$ . Then, by definition, there exists  $r \in \mathbb{Z}$ , such that  $d_1 = d_2 r$ , so  $d_2 | d_1$ . Now let us prove the converse: suppose  $d_2 | d_1$ . Then  $d_1 = d_2 r$  for some  $r \in \mathbb{Z}$ . Then  $d_1 \in I_2$ , but then, since  $I_2$  is an ideal, the whole ideal generated by  $d_1$  is also contained in  $I_2$  (see problem 6 from 3.6, discussed in the previous problem set).

2. Let  $I \subset R$  be an ideal in a ring  $R$ , and let  $\pi : R \rightarrow R/I$  be the canonical projection from the ring to the quotient ring (by definition,  $\pi(x) = x + I$ ).

Prove that  $J \mapsto \pi(J)$  is a bijection between the ideals  $J$  in  $R$  containing  $I$ , and the ideals in  $R/I$ .

**Solution.** Everywhere in this problem, I will denote the elements of the quotient ring by  $r + I, \lambda + I$ , etc., meaning that  $r, \lambda, \dots$  denote the elements of  $R$ .

Recall Problem 30 from Section 2.11, discussed in Homework 5. Let us forget for a moment the multiplication operation, and think of  $R$  as a group with respect to addition (I will write  $(R, +)$  to emphasize this), then  $I$  is a normal subgroup. The ring quotient  $R/I$  is the same set as the group quotient  $(R/I, +)$  (the only difference is that in the case of rings, we also have the operation of multiplication). We know from Problem 30 in 2.11 that the map  $J \mapsto \pi(J)$  is a bijection between subgroups of  $(R, +)$  and subgroups of  $(R/I, +)$ . Since every ideal, by definition, is a subgroup of  $(R, +)$ , the only thing that we still need to prove, is that if  $J$  is an ideal containing  $I$ , then  $\pi(J)$  satisfies the second condition from the definition of an ideal in  $R/I$ , and if  $K$  is an ideal in  $R/I$ , then  $\pi^{-1}(K)$  satisfies the second condition from the definition of an ideal in  $R$ . Thus, we need to prove two things:

- If  $J \supseteq I$  is an ideal,  $\lambda + I \in \pi(J)$ , and  $r + I \in R/I$ , then  $(r + I)(\lambda + I) \in \pi(J)$ .
- If  $K \subset R/I$  is an ideal, and  $\lambda \in \pi^{-1}(K)$ , then for any  $r \in R$ ,  $r\lambda \in \pi^{-1}(K)$ . Note that  $\pi^{-1}(K)$  contains  $I$ , since  $I = \pi^{-1}(0 + I)$  (see problem 30 in 2.11 for a more detailed explanation of this point, if needed).

I will only prove the second statement, the first one is similar and easier. We need to show that  $r\lambda \in \pi^{-1}(K)$ , which is equivalent to  $\pi(r\lambda) \in K$ . We know from class that  $\pi$  is a ring homomorphism, so

$\pi(r\lambda) = \pi(r)\pi(\lambda)$ . Since  $\lambda \in \pi^{-1}(K)$ , we know that  $\pi(\lambda) = \lambda + I \in K$ . Since  $K$  is an ideal in  $R/I$ , and  $\pi(r)$  is an element in  $R/I$ , we have  $\pi(r)\pi(\lambda) \in K$ , and the proof is finished.

**3.** Prove that a ring  $R$  is a field iff  $R$  has only two ideals:  $\{0\}$  and  $R$ .

**Solution.** Suppose that  $\{0\}$  and  $R$  are the only ideals in  $R$ . We want to prove that every nonzero element of  $R$  has an inverse. Let  $x \in R$ ,  $x \neq 0$ . Consider the ideal  $\langle x \rangle$  generated by  $x$ . Since it is not the zero ideal, it must be the whole ring  $R$ , and in particular, it contains 1. Then there exists  $r \in R$ , such that  $rx = 1$ , which means that  $x$  has an inverse.

Conversely, suppose  $R$  is a field, and let  $I \neq \{0\}$  be an ideal. Then there exists some nonzero element  $y$  in  $I$ . Since  $R$  is a field, there exists  $y^{-1}$ , and then  $1 = y^{-1}y \in I$ , so  $I$  contains 1, and therefore  $I = R$ .

**4.** Let  $R$  and  $S$  be rings with identities  $1_R$  and  $1_S$ , respectively. Let  $\phi: R \rightarrow S$  be a nonzero map satisfying  $\phi(x + y) = \phi(x) + \phi(y)$ , and  $\phi(xy) = \phi(x)\phi(y)$ .

(a) Prove that if  $\phi(1_R) \neq 1_S$ , then  $\phi(1_R)$  is a zero-divisor in  $S$ .

**Solution.** Let  $\phi(1_R) = a \in S$ . Note that  $1_R^2 = 1_R$ , so  $\phi(1_R^2) = \phi(1_R) = a$ . Since  $\phi$  is a homomorphism,  $\phi(1_R^2) = \phi(1_R)^2 = a^2$ . So we get:  $a^2 = a$ , i.e.  $a^2 - a = 0_S$ . Since  $S$  has the identity  $1_S$ ,  $a^2 - a = a(a - 1_S)$ . Finally, we have  $a(a - 1_S) = 0$ . Then there are three options:

1.  $a = 0$  – in this case,  $\phi$  is a zero homomorphism (for every  $r \in R$ ,  $\phi(r) = \phi(r \cdot 1_R) = \phi(r) \cdot 0_S = 0_S$ ). Since we assumed that  $\phi$  is nonzero, this option is impossible.

2.  $a - 1_S = 0$ . Then  $a = 1_S$  – and we assumed it's not so.

3.  $a$  and  $a - 1_S$  are both nonzero. That implies that  $a$  is a zero divisor, by definition of zero divisor.

(b) Find an example of  $\phi$ ,  $R$ , and  $S$ , when  $\phi(1_R)$  is a zero-divisor in  $S$ .

For example, take  $R = \mathbb{Z}/2\mathbb{Z}$ ,  $S = \mathbb{Z}/6\mathbb{Z}$ ,  $\phi: R \rightarrow S$  defined by  $\phi(0) = [0]$ ,  $\phi(1) = [3]$  (I'm using the notations  $[\cdot]$  for elements of  $\mathbb{Z}/6\mathbb{Z}$ , and just 0, 1 for the two elements of  $\mathbb{Z}/2\mathbb{Z}$ ). I am skipping the check that  $\phi(ab) = \phi(a)\phi(b)$ , but you had to include it.

**5.** Let  $R$  and  $S$  be commutative rings, and  $R \neq \{0\}$ . Let  $\phi: R \rightarrow S$  be a ring isomorphism.

- (a) Prove that the set of zero divisors in  $S$  is equal to the set  $\{\phi(r) \mid r \text{ is a zero divisor in } R\}$  (i.e. it is the image of the set of zero divisors in  $R$ ).
- (b) Assume that  $R$  and  $S$  have identities  $1_R$  and  $1_S$ , respectively. Let  $S^*$  be the set of units in  $S$ ,  $R^*$  – the set of units in  $R$ . Prove that  $S^* = \phi(R^*)$ .

**Solution.** First, observe that if  $\phi$  is an isomorphism, if  $r \neq 0_R$ , then  $\phi(r) \neq 0_S$ . The reason is that we know that  $\phi(0_R) = 0_S$ , and since  $\phi$  is by definition injective, no other element can be mapped to  $0_S$ .

Now we are ready to prove part (a). Let  $r$  be a zero divisor. That means, exists  $a \in R$  such that  $a \neq 0_R$  and  $ra = 0_R$ . Then  $0_S = \phi(0_R) = \phi(ra) = \phi(r)\phi(a)$ . We just proved that  $\phi(r) \neq 0$ ,  $\phi(a) \neq 0$ , so  $\phi(r)$  is a zero divisor. This proves that the image of the set of zero divisors in  $R$  is contained in the set of zero divisors in  $S$ . We must also prove the opposite inclusion: that if  $s \in S$  is a zero divisor, then there exists  $r \in R$  such that  $r$  is a zero divisor and  $\phi(r) = s$ .

Proof: By definition of zero divisor, exists  $b \in S$  such that  $sb = 0_S$ ,  $b \neq 0_S$ . The map  $\phi$  is surjective, by definition. Then there exist (and unique because  $\phi$  is also injective!)  $r \in R$ ,  $a \in R$  such that  $\phi(r) = s$ ,  $\phi(a) = b$ . Then:  $\phi(ra) = \phi(r)\phi(a) = sb = 0_S$ . But the only element of  $R$  that gets mapped to  $0_S$  is  $0_R$ . Then  $ra = 0_R$ , so  $r$  is a zero divisor.

Part (b) is proved very very similarly.

**6.** Let  $R = \mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}$ .

Let  $I = \{a + b\sqrt{5} \in R \mid a - b \text{ is divisible by } 4\}$ .

- (a) Prove that  $I$  is an ideal of  $R$ .

We need to check that  $I$  is closed under taking differences, and that  $(a + b\sqrt{5})(c + d\sqrt{5}) \in I$  if  $4 \mid a - b$  and  $c, d$  are arbitrary integers. I'm sure everyone did that.

- (b) Prove that the map  $\phi: R \rightarrow \mathbb{Z}/4\mathbb{Z}$  defined by  $\phi(a + b\sqrt{5}) = a - b + \langle 4 \rangle$  (where  $a - b + \langle 4 \rangle$  is the congruence class of the number  $a - b$  in  $\mathbb{Z}/4\mathbb{Z}$ ) is a homomorphism.

We need to check that  $\phi((a + I) + (b + I)) = \phi(a + b + I)$ , and  $\phi((a + I)(b + I)) = \phi(ab + I)$ , where  $a, b$  are elements of  $R$ , so  $a = x + y\sqrt{5}$ ,  $b = x' + y'\sqrt{5}$ ,  $x, x', y, y' \in \mathbb{Z}$ .

Checking:  $(x + y\sqrt{5}) + (x' + y'\sqrt{5}) = (x + x') + (y + y')\sqrt{5}$  by definition of addition in  $R$ . So,  $\phi(a + b + I) = (x + x') - (y + y') + \langle 4 \rangle = (x - x') + (y - y') + \langle 4 \rangle = \phi((a + I) + (b + I))$ . Note that we used the definition of addition in  $\mathbb{Z}/4\mathbb{Z}$  and the fact that it is well-defined. The fact that  $\phi$  preserves multiplication is proved similarly.

- (c) Prove that  $R/I$  is isomorphic to  $\mathbb{Z}/4\mathbb{Z}$ .

All one needs to do here is use the Isomorphism Theorem: We proved above that  $\phi : R \rightarrow \mathbb{Z}/4\mathbb{Z}$  is a homomorphism. Note that it is surjective: for every element in  $c \in \mathbb{Z}/4\mathbb{Z}$  there exist elements  $a + b\sqrt{5}$  in  $R$  with  $a - b \equiv c \pmod{4}$ . By definition of  $I$  and  $\phi$ , the ideal  $I$  is the kernel of  $\phi$ : it consists of the elements  $r$  such that  $\phi(r) = 0$ . Then by the Isomorphism Theorem,  $R/I$  is isomorphic to  $\mathbb{Z}/4\mathbb{Z}$ .

(In particular,  $R/I$  has only 4 elements!)

- (d) Describe the set of zero divisors in  $R/I$ .  
 (e) Describe the set of units  $(R/I)^*$  in  $R/I$ .

For the parts (d), (e), we need to use the previous problem, and part (c):  $R/I$  is isomorphic to  $\mathbb{Z}/4\mathbb{Z}$ ; the the set of units in  $R/I$  is the preimage under this isomorphism of the set of units in  $\mathbb{Z}/4\mathbb{Z}$ . The same holds for zero divisors.  $\mathbb{Z}/4\mathbb{Z}$  has two units: [1] and [3]. The inverse image of [1] in  $R/I$  is the congruence class (coset)  $a + I$  where  $a = x + y\sqrt{5}$  with  $x - y \equiv 1 \pmod{4}$  (any such element would work, of course, because they are all representatives of the same congruence class). The other unit in  $R/I$  is the class  $b + I$  where  $b = x' + y'\sqrt{5}$  with  $x' - y' \equiv 3 \pmod{4}$ .

The ring  $\mathbb{Z}/4\mathbb{Z}$  had one zero divisor: [2]. So, the ring  $R/I$  has one zero divisor: the congruence class  $c + I$  with  $c = x'' + y''\sqrt{5}$ ,  $x'' - y'' \equiv 2 \pmod{4}$ .

**7.** Problem 23 from Section 3.6: Prove that a finite domain  $F$  has to be a field.

**Proof.** Let  $x \neq 0$  be an arbitrary element of  $F$ . Consider the map  $f_x : F \rightarrow F$  defined by the formula  $f_x(y) = xy$  (you may remember that we considered such maps in the beginning of the course, when we studied groups). The plan is to prove that  $F$  is a domain implies that this map has to be injective. The next step, then, would be to say that an injective map from  $F$  to itself has to be also surjective, since  $F$  is finite. And if this map is surjective, it means that there exists  $y_0 \in F$  such that  $f_x(y_0) = 1$ , that is,  $xy_0 = 1$ , which means that  $y_0$  is the inverse of  $x$ . So, the last thing we need to prove is that  $f_x$  is an injective map. Suppose  $f_x(a) = f_x(b)$  for some  $a, b \in F$ . Then  $xa = xb$ , and  $x(a - b) = 0$ . Since there are no zero divisors in  $F$ , and since  $x \neq 0$ , we get  $a - b = 0$ , so  $a = b$ .