

**Problem Set 8. Due Thursday, November 12.**

**From Section 3.6:** Problems 5, 6, 8, 11, 13, 15(i).

**3.6, # 5.** We need to use the definition of an ideal: first, we have to prove our set  $I$  is a subgroup with respect to addition (the quickest way to do it is to prove that for every  $x, y \in I$ , we have  $x - y \in I$  (recall the general criterion for checking whether  $H$  is a subgroup of  $G$ :  $H$  is a subgroup iff  $xy^{-1} \in H$  for every  $x, y \in H$ ). Second, we need to check that if  $r \in I$ , then for every  $\lambda \in R$ , we have  $\lambda r \in I$ .

Subgroup: Let  $x = \lambda_1 r_1 + \cdots + \lambda_n r_n \in I$ ,  $y = \mu_1 r_1 + \cdots + \mu_n r_n \in I$ . Then

$$x - y = (\lambda_1 - \mu_1)r_1 + \cdots + (\lambda_n - \mu_n)r_n \in I.$$

Products: let  $x = \lambda_1 r_1 + \cdots + \lambda_n r_n \in I$ , let  $\mu \in R$ . Then

$$\mu x = (\mu\lambda_1)r_1 + \cdots + (\mu\lambda_n)r_n \in I.$$

**3.6, #6. Comment.** The point of this and the previous problem, combined together, is that *the ideal  $\langle r_1, \dots, r_n \rangle$  is the smallest ideal that contains the elements  $r_1, \dots, r_n$ .* Now, let us prove that if  $r_1, \dots, r_n \in I$ , and  $I$  is an ideal, then  $\langle r_1, \dots, r_n \rangle \subseteq I$ . That means, we need to show that for any  $\lambda_1, \dots, \lambda_n \in R$ , the element  $\lambda_1 r_1 + \cdots + \lambda_n r_n \in I$ . By definition of an ideal, since  $r_i \in I$ , every element  $\lambda_i r_i$  is also in  $I$ , for  $i = 1, \dots, n$ . Now, since an ideal has to be a subgroup with respect to addition, the sum  $\lambda_1 r_1 + \cdots + \lambda_n r_n$  also has to be in  $I$ .

**3.6, #8.** I'll skip (i), (ii), because these are done by direct application of the definition of an ideal, similarly to what we did above, and similarly to (iii) below.

(iii). We need to check two properties: that  $IJ$  is a subgroup of  $R$  with respect to addition, and that for every  $x \in IJ$ ,  $\lambda \in R$ , we have  $\lambda x \in IJ$ .

Subgroup: let  $x = \sum_{i=1}^n a_i b_i \in IJ$ ,  $y = \sum_{i=1}^m c_i d_i \in IJ$ . Then

$$x - y = \sum_{i=1}^n a_i b_i + \sum_{i=1}^m (-c_i) d_i.$$

Since  $I$  is an ideal, and  $c_i \in I$ , we have  $-c_i \in I$ , for  $i = 1, \dots, m$ . Now we see that the expression  $x - y$  is again of the same form as  $x$  and  $y$ : it is a sum of  $n + m$  terms, and each term is a product of an element of  $I$  and an element of  $J$ , so by definition of the set  $IJ$ , it is an element of  $IJ$ .

*Notice that this complicated-looking definition for  $IJ$  was needed because if we just defined  $IJ$  as the set  $\{ab \mid a \in I, b \in J\}$ , we would not have got a subgroup with respect to addition (this is discussed below in Part (v)).*

Products:

$$\lambda x = \sum_{i=1}^n (\lambda a_i) b_i.$$

Since  $I$  is an ideal, and  $a_i \in I$ , then  $\lambda a_i \in I$ , and therefore  $\lambda x \in IJ$ .

(iv). Let us prove that  $IJ \subseteq I \cap J$ . This means, we need to show that  $IJ \subseteq I$  and  $IJ \subseteq J$ . By definition, elements of  $IJ$  are sums of products of the form  $a_i b_i$ , where  $a_i \in I$ ,  $b_i \in J$ . Since  $b_i \in J$ , and  $J$  is an ideal, we have  $a_i b_i \in J$ , and since  $a_i \in I$ , and  $I$  is an ideal, we have also  $a_i b_i \in I$ . So, each of the terms is in both  $I$  and  $J$ . Then, since both  $I$  and  $J$  are subgroups with respect to addition, each element of  $IJ$  has to be both in  $I$  and  $J$ .

Example when  $IJ \neq I \cap J$ : Let  $R = \mathbb{Z}$ ,  $I = J = \langle 2 \rangle$ . Then  $IJ$  consists of numbers that are divisible by 4, so  $IJ \subseteq \langle 4 \rangle$ , in particular,  $2 \notin IJ$ , whereas  $I \cap J = \langle 2 \rangle$ .

(v). This should not be an ideal, because there is no good reason for this set to be a subgroup with respect to addition. However, to make this a rigorous argument, we need an example of  $R$ ,  $I$ , and  $J$ , where the set  $M = \{ab \mid a \in I, b \in J\}$  is not an ideal.

The difficulty in making this example is that if  $R$  is a PID, this won't work. Let us take  $R = \mathbb{Z}[x]$ ,  $I = J = \langle 2, x \rangle$ . I want to show that the set  $M = \{ab \mid a \in I, b \in J\}$  is not a subgroup with respect to addition. For that, it is sufficient to find two elements of  $M$  such that their sum is not in  $M$ . The element  $2 \cdot 2 = 4$  is in  $M$ , and the element  $x \cdot x = x^2$  is in  $M$ . Let us show that  $4 + x^2$  is not in  $M$ . If this was an element of  $M$ , then there would exist two polynomials  $f(x), g(x) \in I$ , such that  $4 + x^2 = f(x)g(x)$ . In particular,  $f$  and  $g$  would have integer coefficients. We know that the polynomial  $x^2 + 4$  cannot be factored (even if you allow real coefficients), unless one of  $f$  and  $g$  is a constant. So, we have  $x^2 + 4 = c(ax^2 + b)$ , and  $a, b, c \in \mathbb{Z}$ . Since  $ca = 1$ , we get  $c = \pm 1$ ; now observe that  $c$  cannot be an element of  $I$ , since neither 1 nor  $-1$  are in  $I$ .

**8.** Let  $f : R \rightarrow S$  be a ring homomorphism. Let us prove that  $\text{Ker } f$  is an ideal. As usual, by definition of the ideal, we need to check that  $x, y \in \text{Ker } f$  implies  $x - y \in \text{Ker } f$ , and  $\lambda x \in \text{Ker } f$  for every  $\lambda \in R$ . So, all we need to check is that  $f(x - y) = 0$ , and  $f(\lambda x) = 0$ . Both of these properties follow right away from the definition of a homomorphism.

Now, let us prove that the image  $f(R)$  is a subring of  $S$ . First, by definition of a homomorphism,  $f(1_R) = 1_S$ , so  $1_S \in f(R)$ . Now, we need to prove that for every  $x, y \in f(R)$ , we have  $xy \in f(R)$  and  $x - y \in f(R)$ . Proof: since  $x, y \in f(R)$ , there exist  $a, b \in R$ , such that  $f(a) = x$ , and  $f(b) = y$ . Then

$$x - y = f(a) - f(b) = f(a - b) \in f(R),$$

and

$$xy = f(a)f(b) = f(ab) \in f(R).$$

**11.** We proved in class that  $\pm 1, \pm i$  are the only units in  $\mathbb{Z}[i]$  (recall that we proved that if  $a + bi$  is a unit, then it must have norm 1, so  $a^2 + b^2 = 1$ ). Now since units always form a group,  $\mathbb{Z}[i]^*$  is a group of 4 elements, and it has an element  $i$  of order 4; therefore it is a cyclic group, and then it is isomorphic to  $\mathbb{Z}/4\mathbb{Z}$ .

**15 (i).** Directly by definition of subring.

**7.** Prove that if  $R$  is a ring, then the zero element 0 is unique, and the neutral element 1 is unique.

By definition, 0 is the neutral element of the group  $(R, +)$  (recall that  $R$  is a group with the operation addition). We know that neutral element in a group is unique.

Now, let us prove that 1 is unique. Suppose there were two elements  $e_1$  and  $e_2$  playing the role of 1 (remember, by definition "1" is such an element that  $1 \cdot x = x$  for every  $x \in R$ ). So, suppose we have two elements satisfying:  $e_1 \cdot x = x \cdot e_1 = x$  for all  $x \in R$ , and  $e_2 \cdot x = x \cdot e_2 = x$  for all  $x \in R$ . Then, plug in  $x = e_2$  in the first equation, and plug in  $x = e_1$  into the second one. We get:  $e_1 e_2 = e_2$ ;  $e_1 e_2 = e_1$ , so  $e_1 = e_2$ , QED.