

**Problem** (Problem 1): Let  $R$  be a ring in which every element  $a$  satisfies  $a^2 = a$ . Show that

- (a)  $2a = 0$  for every  $a \in R$ , so  $a = -a$ ;
- (b)  $R$  is commutative.

**Solution:**

- (a) Let  $a \in R$ . We see that, since  $a + a \in R$ ,  $(a + a)^2 = a + a$ , so that

$$\begin{aligned} a + a &= (a + a)^2 \\ &= (a + a)(a + a) \\ &= a^2 + a^2 + a^2 + a^2 \\ &= a + a + a + a, \end{aligned}$$

and since  $R$  is a ring, we see that  $a + a = 0$ , or that  $a = -a$ .

- (b) Similarly, if  $a, b \in R$ , then since  $(a + b)^2 = a + b$ , we have

$$\begin{aligned} a + b &= (a + b)^2 \\ &= (a + b)(a + b) \\ &= a^2 + b^2 + ab + ba \\ &= a + b + ab + ba, \end{aligned}$$

so  $ab = -ba$ , but since  $-ba = ba$  by the previous part, we have  $ab = ba$ , and so  $R$  is commutative.

**Problem** (Problem 2): Let  $R$  be a ring with identity, and let  $R^\times$  be the set of invertible elements of  $R$ . Show that  $R^\times$  is a group under multiplication. What is  $\mathbb{Z}[i]^\times$ .

**Solution:** First,  $R^\times$  is nonempty, as  $R$  contains a multiplicative identity. Next, if  $a, b \in R^\times$ , we see that  $ab$  admits the inverse  $b^{-1}a^{-1}$ , as

$$\begin{aligned} (ab)(b^{-1}a^{-1}) &= a(bb^{-1})a^{-1} \\ &= aa^{-1} \\ &= 1, \end{aligned}$$

and similarly,

$$\begin{aligned} (b^{-1}a^{-1})(ab) &= b^{-1}(a^{-1}a)b \\ &= b^{-1}b \\ &= 1, \end{aligned}$$

so  $R^\times$  is closed under multiplication. Similarly, since  $(b^{-1})^{-1} = b$  for any  $b \in R^\times$ , every element of  $R^\times$  has a multiplicative inverse, so  $R^\times$  is a group.

To understand the picture of  $\mathbb{Z}[i]^\times$ , we try to understand when, given  $a + bi \in \mathbb{Z}[i]$ ,  $\frac{1}{a+bi} \in \mathbb{Z}[i]$ . Doing the hand calculations, we see that

$$\frac{1}{a + bi} = \frac{1}{a^2 + b^2}(a - bi).$$

Therefore, we see that this holds if and only if  $a = \pm 1$  and  $b = 0$ , or  $b = \pm 1$  and  $a = 0$ , meaning that  $\mathbb{Z}[i]^\times = \{1, i, -1, -i\}$ .

**Problem** (Problem 3): Fix an integer  $n > 1$ . Recall that for  $a, b \in \mathbb{Z}$ , we write  $a \equiv b$  modulo  $n$  if  $a - b$  is divisible by  $n$ . Show that this relation is an equivalence relation on  $\mathbb{Z}$ . Furthermore, show that if  $a \equiv b$

modulo  $n$ , and  $c \equiv d$  modulo  $n$ , then

$$a + c \equiv b + d \text{ modulo } n, \text{ and } ac \equiv bd \text{ modulo } n.$$

**Solution:** Since 0 is divisible by  $n$ , it is clear that  $a \equiv a$  modulo  $n$ , so the relation is reflexive.

If  $a \equiv b$  modulo  $n$ , then since  $n|(a - b)$ , we must also have  $n|(b - a)$ , so  $b \equiv a$  modulo  $n$ , so the relation is symmetric.

Finally, if  $a \equiv b$  modulo  $n$  and  $b \equiv c$  modulo  $n$ , then since  $n|a - b$  and  $n|b - c$ , by adding, we see that  $n|(a - b) + (b - c)$ , so  $n|a - c$  and  $a \equiv c$  modulo  $n$ , so the relation is transitive.

Now, if  $a \equiv b$  modulo  $n$ , and  $c \equiv d$  modulo  $n$ , then since  $n|(a - b)$  and  $n|(c - d)$ , by adding, we see that  $n|(a + c) - (b + d)$ , so  $a + c \equiv b + d$  modulo  $n$ . To see the last equivalence, we rewrite  $a = b + kn$ ,  $c = d + \ell n$ , where  $k, \ell \in \mathbb{Z}$ . Thus, multiplying things out, we see that

$$\begin{aligned} ac &= (b + kn)(d + \ell n) \\ &= bd + nkd + \ell nb + k\ell n^2 \\ &= bd + (kd + \ell b + k\ell n)n, \end{aligned}$$

and since  $kd + \ell b + k\ell n \in \mathbb{Z}$ , we have  $ac \equiv bd$  modulo  $n$ .

**Problem (Problem 4):** Show that a finite commutative ring with 1 and without zero divisors is a field.

**Solution:** Let  $a \in R$ , and consider the map  $\varphi_a: R \setminus \{0\} \rightarrow R \setminus \{0\}$  given by  $b \mapsto ab$ . We see that if  $ab = ac$ , then  $a(b - c) = 0$ , and since  $a \neq 0$ , we see that  $b = c$ , so  $\varphi_a$  is injective. Since  $\varphi_a$  is an injective self-map of a finite set,  $\varphi_a$  is surjective, so  $\varphi_a$  is bijective, and thus  $\varphi_a^{-1}(1)$  is well-defined, so  $a\varphi_a^{-1}(1) = 1$ , meaning  $a$  has a right-inverse. Since  $R$  is commutative, we have  $\varphi_a^{-1}(1)a = 1$ , so  $R$  is a field.

**Problem (Problem 5):** Let  $R = \text{Mat}_n(\mathbb{R})$  be the ring of real  $n \times n$  matrices. Show that if  $A$  satisfies  $\det(A) = 0$ , then there exist nonzero  $B, C \in R$  such that  $AB = 0_n$  and  $CA = 0_n$ .

**Solution:** If  $A$  is the zero matrix, then the problem is trivial, so we assume the matrix is not the zero matrix. We notice that, since 0 is an eigenvalue of  $A$ , as can be seen by plugging in 0 for the characteristic polynomial of  $A$ , the minimal polynomial  $m_A(t)$  factors as  $m_A(t) = tp(t)$  for some monic polynomial  $p \in \mathbb{R}[t]$  with strictly lesser degree than  $m_A(t)$ . Since  $m_A(t)$  is the minimal polynomial of  $A$ , it must mean that  $p(A) \neq 0$ , so by setting  $B = p(A)$ , since  $A$  commutes with all powers of itself, we see that  $AB = BA = 0$ .

**Problem (Problem 6):** An element  $x \in R$  is called *nilpotent* if there exists  $n > 0$  such that  $x^n = 0$ .

Assume  $R$  is a commutative ring with identity. Show that if  $x \in R$  is nilpotent, then

(a)  $rx$  is nilpotent for any  $r \in R$ ;

(b)  $1 + x$  is invertible.

**Solution:**

(a) We see that, since  $R$  is commutative,

$$\begin{aligned} (rx)^n &= (rx)(rx) \cdots (rx) \\ &= r^n x^n \\ &= 0, \end{aligned}$$

so  $rx$  is nilpotent.

(b) We see that if  $a$  is nilpotent, then

$$1 = 1 - a^n$$

$$= (1 - a)(1 + a + \cdots + a^{n-1}),$$

meaning that  $1 - a$  is invertible. Furthermore, we note that if  $a$  is nilpotent, then so is  $-a$ , as  $-a = (-1)a$ , allowing us to apply part (a). Thus,  $1 + x = 1 - (-x)$  is invertible if  $x$  is nilpotent.

**Problem** (Problem 7): Let  $R = \text{Mat}_n(\mathbb{F})$ , where  $\mathbb{F}$  is a field. Show that if  $I$  is a nonzero 2-sided ideal of  $R$ , then  $I = R$ .

**Solution:** We show that if  $I$  is a nonzero two-sided ideal in  $\text{Mat}_n(\mathbb{F})$ , then  $I_n \in I$ .

Since  $I$  is nonzero, there is some matrix  $(a_{ij})_{i,j} \in I$  such that at particular indices  $i_0$  and  $j_0$ ,  $a_{i_0 j_0} \neq 0$ . Since  $a_{ij} \in \mathbb{F}$  for all  $i, j$ , we have that  $a_{i_0 j_0}^{-1}$  exists.

Let  $e_{ij}$  be the matrix unit with a position 1 at index  $(i, j)$  and zero elsewhere. Then, via some matrix algebra, we see that

$$a_{i_0 j_0} e_{kk} = e_{k i_0} a e_{j_0 k}$$

which is necessarily in  $I$ , as  $I$  is a two-sided ideal. Therefore, since  $\mathbb{F}$  is a field, we see that  $(e_{kk})_{i,j} \in I$  for each  $k$ , so  $\sum_{k=1}^n (e_{kk})_{i,j} \in I$ , so  $I_n \in I$ , meaning  $I = R$ .

**Problem** (Problem 8): Let  $n \in \mathbb{N}$  and consider  $\mathbb{Z}^n$  as a ring with component-wise addition and multiplication.

(a) Prove that  $\text{aut}_{\text{group}}(\mathbb{Z}^n) \cong \text{GL}_n(\mathbb{Z})$ .

(b) Prove that  $\text{aut}_{\text{ring}}(\mathbb{Z}^n) \cong \text{Sym}(n)$ .

**Solution:** Before we start, we first notice that every element of  $\mathbb{Z}^n$  can be written as

$$v = a_1 e_1 + a_2 e_2 + \cdots + a_n e_n,$$

where  $e_j$  are the standard basis of  $\mathbb{Z}^n$  and  $a_j \in \mathbb{Z}$  for each  $j$ . Therefore, if  $\varphi$  is any automorphism as either a group or a ring, we may write  $\varphi(v)$  as some integer linear combination of  $\varphi(e_j)$ , where the  $e_j$  are the standard basis vectors for  $\mathbb{Z}^n$ .

(a) Let  $\varphi \in \text{aut}_{\text{group}}(\mathbb{Z}^n)$ . If  $v \in \mathbb{Z}^n$  is some vector, then

$$\begin{aligned} \varphi(v) &= \varphi(a_1 e_1 + a_2 e_2 + \cdots + a_n e_n) \\ &= a_1 \varphi(e_1) + a_2 \varphi(e_2) + \cdots + a_n \varphi(e_n). \end{aligned}$$

Since a linear transformation may be specified uniquely via a basis, we may specify a matrix element  $A_\varphi \in \text{Mat}_n(\mathbb{Z})$  by

$$A_\varphi e_j = \varphi(e_j)$$

for each  $j$ . Note that since each  $\varphi$  is invertible, each  $A_\varphi$  may have  $A_\varphi^{-1}$  defined by  $A_\varphi^{-1} e_j = \varphi^{-1}(e_j)$ , so each  $A_\varphi \in \text{GL}_n(\mathbb{Z})$ . Similarly, we see that if  $\psi, \varphi \in \text{aut}_{\text{group}}(\mathbb{Z}^n)$ , then

$$\begin{aligned} \psi \circ \varphi(e_j) &= A_\psi(\varphi(e_j)) \\ &= A_\psi(A_\varphi e_j) \\ &= A_\psi A_\varphi e_j. \end{aligned}$$

Therefore, the map  $\varphi \mapsto A_\varphi$  is an isomorphism, so  $\text{aut}_{\text{group}}(\mathbb{Z}^n) \cong \text{GL}_n(\mathbb{Z})$ .

(b) Let  $\varphi \in \text{aut}_{\text{ring}}$ ; notice that  $\text{aut}_{\text{ring}} \subseteq \text{aut}_{\text{group}}$  meaning that we know already that  $\varphi$  can be written as some element of  $\text{GL}_n(\mathbb{Z})$ . Suppose that, for some  $e_k$ , we may write

$$\varphi(e_k) = \sum_{k=1}^n a_k e_k.$$

Notice then that, since  $e_i e_j = \delta_{ij}$ , where  $\delta_{ij}$  is the Kronecker delta symbol, we get

$$\begin{aligned}\varphi(e_k^2) &= \varphi(e_k)\varphi(e_k) \\ &= \sum_{k=1}^n a_k^2 e_k \\ &= \sum_{k=1}^n a_k e_k,\end{aligned}$$

meaning in particular that  $a_k = 0$  or  $a_k = 1$ , seeing as the  $a_k$  are elements of  $\mathbb{Z}$ .

If  $\varphi(e_k) = e_{k_1} + \cdots + e_{k_i}$  and  $\varphi(e_\ell) = e_{\ell_1} + \cdots + e_{\ell_j}$ , then

$$\begin{aligned}\varphi(e_k e_\ell) &= (e_{k_1} + \cdots + e_{k_i})(e_{\ell_1} + \cdots + e_{\ell_j}) \\ &= \sum_{m=1}^i \sum_{n=1}^j e_{k_m} e_{\ell_n} \\ &= \sum_{m=1}^i \sum_{n=1}^j \delta_{k_m \ell_n} e_{k_m}\end{aligned}\tag{*}$$

Yet, since  $\varphi(0) = 0$ , we have  $e_k e_\ell = \delta_{k\ell} e_k = \delta_{k\ell} e_\ell$ , meaning

$$\begin{aligned}\varphi(e_k e_\ell) &= \delta_{k\ell} \varphi(e_k) \\ &= \delta_{k\ell} (e_{k_1} + \cdots + e_{k_i}) \\ &= \delta_{k\ell} \varphi(e_\ell) \\ &= \delta_{k\ell} (e_{\ell_1} + \cdots + e_{\ell_j}).\end{aligned}\tag{†}$$

Now, notice that the expression in (\*) can pick out at most one basis vector, and that this basis vector depends on the equivalence of  $i$  and  $j$ , following from (†) and (‡).

Thus, for any standard basis vector  $e_i$ ,  $\varphi(e_i) = e_j$  for some  $j$ . Furthermore, no distinct  $e_i$  and  $e_j$  can map to the same element, or else we would get  $\varphi(e_i e_j) = 0 = e_k$ , which is a contradiction. Thus, the map  $\{e_1, \dots, e_n\} \rightarrow \{\varphi(e_1), \dots, \varphi(e_n)\}$  is an injective self-map of a finite set, hence surjective, so it is a permutation of  $\{1, \dots, n\}$ . Thus,  $\text{aut}_{\text{ring}}(\mathbb{Z}^n) \cong S_n$ .