

## TRAINING MIDTERM 1 // SOLUTIONS

1.– On the set  $\{T, F\}$ , we consider three binary laws:

- (i) AND is defined by:  $x \text{ AND } y = T$  if and only if  $x = y = T$ .
- (ii) OR is defined by:  $x \text{ OR } y = T$  if and only if at least one of  $x$  or  $y$  is  $T$ .
- (iii) XAND is defined by  $x \text{ XAND } y = T$  if and only one exactly one among  $x, y$  is  $T$ .

a.– Which of those laws are group laws?

b.– Among those laws, are there two that are isomorphic to each other? If yes tell which ones, and describe an isomorphism.

**Solution:** AND and OR are not group laws. There are many correct ways to prove this. One is as follows : in a group, there can be only one solution of the equation  $x * x = x$  : the neutral element. But in  $(\{T, F\}, \text{AND})$  we have  $T \text{ AND } T = T$  and  $F \text{ AND } F = F$ . Therefore this is not a group. And the same argument works for OR.

XAND is a group. The shortest way to see it is to construct an isomorphism  $(\{T, F\}, \text{XAND})$  to  $\mathbb{Z}_2$  : send  $T$  to  $\bar{0}$  and  $F$  to  $\bar{1}$

Therefore, XAND is not isomorphic to any of the others. But OR and AND are isomorphic, and it is easy to describe an isomorphism between them: the negation that sends  $T$  to  $F$  and  $F$  to  $T$ .

2.– Let  $\tau \in S_n$  and assume that  $\tau^2 = e$ . Show that all orbits of  $\tau$  have cardinality either 1 or 2.

**Solution:** The orbit of an element  $x$  is the set of all  $\tau^n(x)$  for  $n \in \mathbb{Z}$ . Since  $\tau^2 = e$ ,  $\tau^n(x)$  is  $x$  if  $n$  is even, and  $\tau(x)$  if  $n$  is odd. Therefore, the orbits has cardinality 1 (if it happens that  $x = \tau(x)$ ) or 2 (otherwise).

3.– Let  $A$  be the set of elements of  $\mathbb{Z}$  of the form  $66a + 12b - 9c$  for  $a, b, c \in \mathbb{Z}$ . Show that  $A$  is a subgroup of  $\mathbb{Z}$ . Is  $A$  cyclic? If yes, give a generator.

Take two elements of  $A$ :  $x = 66a + 12b - 9c$  and  $y = 66a' + 12b' - 9c'$ , with  $a, b, c, a', b', c'$  in  $\mathbb{Z}$ . Then  $x - y = 66(a - a') + 12(b - b') - 9(c - c')$  is also in  $A$ . This suffices to show that  $A$  is a subgroup of  $\mathbb{Z}$ . By a theorem seen in class, all subgroups of  $\mathbb{Z}$  is cyclic; therefore so is  $A$ . To find a generator, we can prove as in class that the gcd of 66, 12, -9, which is 3 will do. Or if this proves seems too difficult, you can guess that the result could be the gcd, that is 3, and prove directly that it is a generator, which is easy : every element of  $A$  is clearly multiple of 3, and  $3 = 66 \times 0 + 12 \times 1 - 9 \times 1$  is in  $A$ .

4.– Let  $A$  be the set of elemnets in  $\mathbb{R}$  of the form  $a + b\sqrt{2}$  for  $a, b \in \mathbb{Z}$ . Show that  $A$  is a subgroup of  $(\mathbb{R}, +)$ . Is  $A$  cyclic? If yes, give a generator.

**Solution:** The proof that  $A$  is a subgroup works as in 3.– But now  $A$  is a subgroup of  $\mathbb{R}$ , not of  $\mathbb{Z}$ , and no theorem in class says that  $A$  is cyclic. Indeed, it is not cyclic, but the proof is a little bit tricky.

Assume by contradiction that  $A$  is cyclic. Let  $g$  be a generator. Then  $g \neq 0$  since  $A \neq 0$ , and if  $g$  is negative,  $-g$  is also a generator, so replacing  $g$  by  $-g$ , we can assume that our generator  $g$  satisfies  $g > 0$ . Therefore, all the positive elements in  $A$  are of the forms  $ng$ ,  $n \in \mathbb{Z}_+$ . In particular, no elements in  $g$  lies strictly between 0 and  $g$

To be continued tomorrow.

5.– How many elements does have the subgroup of  $(\mathbb{C}^*, \times)$  generated by  $i$ ? Is it cyclic?

**Solution:** It has 4 elements:  $i$ ,  $-1$ ,  $-i$ ,  $1$ . It is cyclic, generated by  $i$  (and  $-i$ ).

6.– Let  $G = \mathbb{Z}_{12}$  and  $S = \{3, 7\}$ . Draw the Cayley graph of  $(G, S)$ . Is  $S$  a generating subset of  $G$ ?

**Solution:** For obvious reasons, I do not draw the Cayley graph. But 7 is relatively prime to 12, so  $\bar{7}$  is a generator of  $\mathbb{Z}_{12}$ . Therefore the subset  $\{\bar{3}, \bar{7}\}$  is generating.

7.– Show that there are three elements in  $A_4$  that are the product of two disjoint transpositions. Show that with the identity, they form a subgroup of  $A_4$  with four elements. Is this subgroup cyclic?

**Solution:** A transposition is determined by its support, which is a subset with two elements in  $\{1, 2, 3, 4\}$ . There are six of them. One can have a first transposition  $\tau_1$ , there is only one transposition  $\tau_2$  with a disjoint support, since this support has to be the complement in  $\{1, 2, 3, 4\}$  of the support of  $\tau_1$ . What we have shown is that there are six ordered pair  $(\tau_1, \tau_2)$  transpositions with disjoint support. But for such an ordered pair,  $\tau_1\tau_2 = \tau_2\tau_1$ , so actually those six pairs give rise to *at most three product of transpositions with disjoint support*. Explicitly  $(12)(34)$ ,  $(13)(24)$ ,  $(14)(23)$ . It remains only to show that those three elements are distinct, which can be checked easily by hand, or which is a consequence of the unicity in the theorem on decomposition into cycles with disjoint support.

Now we consider the set  $K = \{e, (12)(34), (13)(24), (14)(23)\}$ . Note that each element  $x$  in this set satisfies  $x^2 = e$ . For example  $((12)(34))^2 = (12)^2(34)^2 = ee = e$ , the first equality following from the fact that  $(12)$  and  $(34)$  commute. Therefore,  $x = x^{-1}$  for all  $x \in K$

To check that  $K$  is a subgroup, it suffices, for all  $x, y \in K$ , to check that  $xy^{-1} = xy$  is in  $K$ . The cases where  $x$  or  $y$  is  $e$ , and the cases where  $x = y$  are obvious. In cases  $x = (12)(34)$  and  $y = (13)(24)$ , one compute  $xy = (14)(23)$ , and the others remaining cases are similar to this one.

Finally,  $K$  is not cyclic, since it has cardinality 4, but all elements satisfy  $x^2 = e$ .

8.– Let  $\sigma \in S_n$  and  $(a_1, \dots, a_m)$  a cycle of  $S_n$ . Is  $\sigma(a_1, \dots, a_m)\sigma^{-1}$  a cycle of  $S_m$ ? if yes, what is its order? What is its support?

**Solution:** We compute easily that  $\sigma(a_1, \dots, a_m)\sigma^{-1} = (\sigma(a_1), \dots, \sigma(a_m))$ , which is another cycle of order  $m$ .

9.– Compute  $(ijk)(kls)$  where  $i, j, k, l, s$  are distinct. Is that a cycle? Otherwise, what is its decomposition as a product of disjoint cycles?

**Solution:** The product  $(ijk)(kls)$  sends  $s \mapsto i$ ,  $l \mapsto s$ ,  $k \mapsto l$ ,  $j \mapsto k$ , and  $i \mapsto j$ . So it is a cycle  $(ijkl s)$ .