Solutions Midterm

1. Examples are
   (a) S_3
   (b) $V_4 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
   (c) $H = 5\mathbb{Z}$, $G = \mathbb{Z}$
   (d) S_3 and $\mathbb{Z}/6\mathbb{Z}$
   (e) The subgroup generated by the reflection y in D_3
   (f) $G = \mathbb{R}$, $H = \mathbb{Z}$, $\mathbb{R}/\mathbb{Z} \simeq S^1$ that is not isomorphic to any subgroup of $\mathbb{R}$
   (g) A subgroup of index 2 is always normal
   (h) $S_3 = \mathbb{Z}/2\mathbb{Z} \ltimes \mathbb{Z}/3\mathbb{Z}$ is not isomorphic to $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

2. Let $[x, y]$ be any commutator element of G. Then
$$\varphi([x, y]) = \varphi(x)\varphi(y)\varphi(x)^{-1}\varphi(y)^{-1} = 1$$
since φ is a homomorphism taking values in an abelian group.

3. D_{12} is not isomorphic to $D_6 \times Z$. Indeed one of the two generators of D_{12} has order 12, but every element h of $D_6 \times Z$ satisfies $h^6 = 1$. To prove this last fact it is enough to remember that an element $(g, h) \in G \times H$ has order the minimum common multiple of the orders of the elements g and h (since g and h commute). Moreover any element z of D_6 satisfies $z^6 = 1$, and the center of D_{12} is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, hence an element of Z has order either 1 or 2.

   • 5 points for the above answer or any correct answer that is correctly elaborated and explained.
   • $4 - 5$ points for the right answer with a descent explanation. The variation from 4 points to 5 points depends on the quality of the arguments presented.
   • $1 - 2$ points for wrong answer with some good statements (Theorems or correct related statements even though the final answer is wrong). The variation from 1 point to 2 points depends on the quality of the arguments presented.
   • 3 points for correct final answer with not very good explanation or a bit poor explanation. Correct explanations nonetheless.
   • $0 - 1$ point for correct final answer but with very poor or wrong explanations. The variation from 0 point to 1 points depends on the quality of the arguments presented. For example, if the final answer is correct but the arguments are completely wrong i.e. it is clear that the student accidentally obtain the correct answer since his line of thought was mistaken, then the problem gets 0 points.

4. Let us consider the action of G on $(\mathbb{Z}/2\mathbb{Z})^2$. There are two orbits for this action: the null vector is a single orbit, the other three vectors form a second orbit O, and G acts on the orbit O as a permutation group. The orbit O consists of the vectors $v_1 = (1,0)$, $v_2 = (0,1)$, $v_3 = (1,1)$. The invertible matrix $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ acts as the permutation $(1,2,3)$, and the matrix $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ acts as the permutation $(1,3)$. Since the permutation $(1,2,3)$ and $(1,3)$ generate S_3, the permutation representation gives a surjective homomorphism $GL_2(\mathbb{Z}/2\mathbb{Z})$. Moreover since $GL_2(\mathbb{Z}/2\mathbb{Z})$ has six elements the homomorphism must be injective, in particular it gives an homomorphism.

5. Let G be a finite subgroup of M_2. Since G is finite, there are only finitely many translation and rotations in G, and this implies that G is a discrete subgroup of M_2. From what was proven in class we have an exact sequence

$$1 \longrightarrow T \longrightarrow G \longrightarrow \overline{G} \longrightarrow 1$$

T is a discrete subgroup of $\mathbb{R}^2$, in particular it is either $\{0\}$, or $\mathbb{Z}$, or $\mathbb{Z}^2$. Since T is a subgroup of G, it is finite, hence it must be $\{0\}$. This implies that G is isomorphic to the point group $\overline{G}$, that is a discrete subgroup of O_2, hence it is either a cyclic group or a dihedral group.
Common errors

(a) The reflections do not form a subgroup of M_2: if you compose two reflection with respect to distinct planes you get rotations (if the planes have a point in common) and translations (if the planes are parallel)

(b) *Discrete* is a property of groups and not of single isometries.

(c) There are finite subgroups of M_2 that are not subgroups of O_2: for example if you fix a point p different from the origin and consider the group of rotations around that point of angle $2\pi/n$ you get a finite group. Indeed this group is conjugate to the cyclic subgroup of order n of O_2 via the translation t_p, but none of its elements, apart from the identity are contained in O_2.

(d) Even if a finite group cannot contain translations, it can still have an element of the form $\rho_\theta t_{-2p}$: indeed this isometry is a rotation around the point p.

Grading scheme The full solution was obviously worth 5 points. In general you would get one point for any of the following: stating that finite groups that fix the origin are precisely C_n and D_n. Realizing that there are finite subgroups of M_2 that are not contained in O_2, showing that a finite group of translations is trivial, or more generally that a finite group cannot contain translations.

6. **Test on Monday** : Show that A_4 has no subgroup of order 6.

The group A_4 contains three double transpositions, eight 3-cycles and the identity :

$$(12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), (143), (234), (243), 1.$$

(Up to 2 points for the structure of A_4, 1 point for noting that A_4 contains double transpositions.)

A group of order 6 is isomorphic to either $\mathbb{Z}_6$ or S_3. We show successively that A_4 has no subgroup that is isomorphic to one of these two groups. (2 points - also if argumenting in terms of generators and their orders.)

First, if there was a subgroup of A_4 isomorphic to $\mathbb{Z}_6$, then A_4 would contain an element of order 6. This is a contradiction. (1 pt)

Second, if a subgroup A_4 is isomorphic to S_3, then each transposition in S_3 must be mapped under the isomorphism to an element of order 2 in A_4. The only element of order 2 are $\tau_1 = (12)(34)$, $\tau_2 = (13)(24)$ and $\tau_3 = (14)(23)$. Note that $\tau_i\tau_j = \tau_j\tau_i$ while transpositions in S_3 do not commute. Hence there is no such isomorphism. (1 pt)

Variant : Assume by contraddiction that A_4 had a subgroup H of order 6. The group H would have an element h_2 of order 2 and an element h_3 of order 3. Since the group A_4 consists of even permutations, the only elements of order 2 of A_4 are the products of two transpositions. In particular, up to renaming the elements, we can assume that $h_2 = (1, 2)(3, 4)$. Moreover h_3 is a 3 cycle and we can assume that h_3 is the element $h_3 = (1, 2, 3)$: indeed, again up to renaming we can assume that h_3 fixes 4, and, since H is a group, both h_3 and h_3^2 are in H, and one of these two elements has the form $(1, 2, 3)$.

We will now show that the subgroup generated by h_3 and h_2 has cardinality bigger than 6. Indeed let us consider the products $h_3h_2 = (1, 2, 3)(1, 2)(3, 4) = (1, 3, 4)$ and $h_2h_3 = (1, 2)(3, 4)(1, 2, 3) = (2, 4, 3)$. Since h_2h_3 is not equal to h_3h_2 nor to $h_3^2h_2 = (2, 3, 4)$, H cannot have 6 elements.

Test on Tuesday : Let H be a non-trivial subgroup of a group G that is contained in every non-trivial subgroup of G. Prove that H is contained in the center Z of G.

Variant 1 : In other words, the statement amounts to proving that G has non-trivial center (1 pt). For each element $g \in G$ distinct from the identity, we consider its centralizer $Z(g) = \{x \in G : xg = gx\}$. This is a non-trivial subgroup of G since it must contain the non-trivial subgroup generated by g. Note that in the special case where G is cyclic, the group is abelian and $Z = G$ contains trivially H. By assumption, H is contained in the intersection

$$\bigcap_{g \in G} Z(g) = Z,$$

where the last equality was given as an easy exercise in class (5 pts).

Variant 2 : The statement could also be proven directly. Let $h \in H$ and $g \in G$. We claim that $gh = hg$, i.e. $h \in Z$. If $g \neq 1$, then the element generates a non-trivial subgroup that contains H by assumption. Note that in the special case where G is cyclic, the group is abelian and $Z = G$ contains trivially H. In particular, $h = g^n$ for some n. The claim follows immediately. (6 pts)

7. Let us recall that $(\mathbb{Z}/m\mathbb{Z})^\times$ denotes the multiplicative group of elements of $\mathbb{Z}/m\mathbb{Z}$ that have a multiplicative inverse and the elements of this group are the congruence classes of integers that are coprime with m. Moreover any element in $(\mathbb{Z}/m\mathbb{Z})^\times$ is a generator of $(\mathbb{Z}/m\mathbb{Z})^+$.

   Let us now define the map

$$\begin{array}{rccc} \Phi: & \mathrm{Aut}(\mathbb{Z}/m\mathbb{Z}) & \to & (\mathbb{Z}/m\mathbb{Z})^\times \\ & f & \mapsto & f(1). \end{array}$$

   Φ is well defined since, if f is an automorphism of $\mathbb{Z}/m\mathbb{Z}$, the image of 1 must be a generator, and bijective since an automorphism of a cyclic group is fully determined by the values it takes on a generator: indeed if f is an automorphism of $\mathbb{Z}/m\mathbb{Z}$, $f(x) = xf(1)$. Moreover from this last equation it follows that $\Phi(gf) = g \circ f(1) = g(f(1)) = f(1)g(1) = g(1)f(1) = \Phi(g)\Phi(f)$, and hence Φ is a group isomorphism.

   If p is prime, any element of $\mathbb{Z}/p\mathbb{Z}$ apart from 0 is a coprime with p, in particular $\mathbb{Z}/p\mathbb{Z}^\times$ has cardinality $p - 1$.

   The group $\mathbb{Z}/8\mathbb{Z}^\times$ is not cyclic. Its elements are 1,3,5,7 with $3 \cdot 3 \equiv 5 \cdot 5 \equiv 7 \cdot 7 \equiv 1$.

   Grading:

   - Proof of the first part – 3 pts including:
     - The image of 1 determines the homomorphism – 1 pt
     - The map $f \mapsto f(1)$ is a homomorphism and an isomorphism – 1 pt
   - Deducing that the cardinality of $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ is $p - 1$ – 1 pt
   - Giving a good (well-understood) example and a correct argument – 1+1 pts