Silvain Rideau silvain.rideau@berkeley.edu
1091 Evans www.normalesup.org/~srideau/en/teaching

Solutions to homework 2

Due September 11th

Problem 1 (Order) **:**

1. Find the order of every element in $(\mathbb{Z}/18\mathbb{Z},+)$ and of every element of $((\mathbb{Z}/18\mathbb{Z})^\star,\cdot)$. (You should start by giving a list of the elements of $\mathbb{Z}/18\mathbb{Z}$ that have a multiplicative inverse; there are six of them).

   Solution: In $(\mathbb{Z}/18\mathbb{Z},+)$:
   - The order of $\overline{0}$ is 1.
   - The order of $\overline{1}$, $\overline{5}$, $\overline{7}$, $\overline{11}$, $\overline{13}$ and $\overline{17}$ is 18 as they are prime with 18.
   - The order of $\overline{2}$, $\overline{4}$, $\overline{8}$, $\overline{10}$, $\overline{14}$ and $\overline{16}$ is 9 as their gcd with 18 is 2.
   - The order of $\overline{3}$ and $\overline{15}$ is 6 as their gcd with 18 is 3.
   - The order of $\overline{6}$ and $\overline{12}$ is 3 as their gcd with 18 is 6.
   - The order of $\overline{9}$ is 2 as its gcd with 18 is 9.

   The six elements of $((\mathbb{Z}/18\mathbb{Z})^\star$ are $\overline{1}$, $\overline{5}$, $\overline{7}$, $\overline{11}$, $\overline{13}$ and $\overline{17}$ (indeed n is prime with 18 if and only if there exists k and $l \in \mathbb{Z}$ such that $nk+18l=1$ i.e. $nk = 1 \mod 18$).
   - $\overline{1}$ has order 1
   - $\overline{17}$ has order 2 since $17^2 \equiv (-1)^2 \equiv 1 \mod 18$.
   - $\overline{7}$ and $\overline{13}$ have order 3 since $7^3 \equiv 49\cdot 7 \equiv -5\cdot 7 \equiv -35 \equiv 1 \mod 18$ and $13^2 \equiv (-5)^3 \equiv 25\cdot(-5) \equiv -7\cdot 5 \equiv 1 \mod 18$ but $7^2 \equiv 49 \equiv 13 \not\equiv 1 \mod 18$ and $13^2 \equiv (-5)^2 \equiv 25 \equiv 7 \not\equiv 1 \mod 18$.
   - Finally, we have $5^2 \equiv 25 \equiv 7 \mod 18$, $11^2 \equiv\equiv (-7)^2 \equiv 49 \equiv 13 \mod 18$ and 7 and 13 have order 3. Moreover $5^3 \equiv (-13)^3 \equiv -(13)^3 \equiv -1 \mod 18$, $5^4 \equiv 25^2 \equiv (7)^2 \equiv 13 \mod 18$, $5^5 \equiv (-13)^5 \equiv -13\cdot(13^2)^2 \equiv 5\cdot 7^2 \equiv 5\cdot(-5) \equiv -25 \equiv 11 \mod 18$, $11^3 \equiv (-7)^3 \equiv -(7)^3 \equiv -1 \mod 18$, $11^4 \equiv 49^2 \equiv (-5)^2 \equiv 7 \mod 18$, $11^5 \equiv (-7)^5 \equiv -7\cdot(7^2)^2 \equiv -7\cdot 13^2 \equiv -7\cdot 7 \equiv -49 \equiv 5 \mod 18$. So $\overline{5}$ and $\overline{11}$ have order 6.

2. Let G be a group, $a, b \in G$. Show that the order of ab is equal to the order of ba.

   Solution: Let n be the order of ab. We have $(ab)^n = 1$ and hence $(ba)^n = b(ab)^n b^{-1} = bb^{-1} = 1$. It follows that the order of ba is smaller than n, Symmetrically , the order of ab is smaller than the order of ba so they must be equal.

3. Let G be a group such that every (non identity) element has order 2. Show that G is abelian.

   Solution: For all $x \in G$, we have $x^2 = 1$ and hence $x = x^{-1}$. It follows that for all $a, b \in G$, $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$ and hence G is Abelian.

Problem 2 (Permutations) **:**

1. Let $\gamma \in S_n$ be an k-cycle. What are the $i \in \mathbb{Z}$ such that γ^i is a k-cycle.

   Solution: Let $\gamma = (a_0 a_1 \dots a_{k-1})$ then $\gamma^i(a_j) = a_{i+j}$ (the indices are taken to be in $\mathbb{Z}/k\mathbb{Z}$). Let us prove that if γ^i is a k-cycle, then $\gcd(i,n) = 1$. If γ^i is a k-cycle then it has order k in $\langle\gamma\rangle$ which has size k and hence $(k,i) = 1$. Conversely, assume $\gcd(i,k) = 1$, and for all $j \in \mathbb{Z}/k\mathbb{Z}$, let $b_j = a_{ij}$ (this is well defined because if $j_2 = j_1 + kd$, then $a_{ij_2} = a_{ij_1+kid} = a_{ij_1}$). Then $\gamma^i(b_j) = b_{j+1}$ and if $x \notin \{a_i : i \in \mathbb{Z}/k\mathbb{Z}\}$, $\gamma(x) = x$ and hence $\gamma^i(x)$. To show that γ^i is a k-cycle, it suffices to show that the b_j are distinct. If $b_{j_1} = b_{j_2}$, then $a_{ij_1} = a_{ij_2}$ and hence $ij_1 = ij_2 \mod k$, i.e. $k|i(j_1 - j_2)$. As $(k,i) = 1$, it follows that $k|(j_1 - j_2)$ and hence $j_1 = j_2 \mod k$. That concludes the proof.

2. Show that every element of S_n can be written as an arbitrary product of the elements (01) and $(01\dots n-1)$ (we say that (01) and $(01\dots n-1)$ generate S_n).

   Solution: Let us first prove the following very useful fact. Let $\gamma = (a_0 a_1 \dots a_{k-1})$ be a k-cycle and $\sigma \in S_n$, then $\gamma_\sigma := \sigma \circ \gamma \circ \sigma^-1 = (\sigma(a_0)\sigma(a_1)\dots\sigma(a_{k-1}))$. Indeed $\gamma_\sigma(\sigma(a_i)) = \sigma \circ \gamma \circ \sigma^-1(\sigma(a_i)) = \sigma \circ \gamma(a_i) = \sigma(a_{i+1})$ and hence (because σ is a permutation, the $\sigma(a_i)$ are distinct), γ_σ is indeed the k-cycle sending $\sigma(a_i)$ to $\sigma(a_{i+1})$.

   Let $\tau = (01)$ and $\gamma = (01\dots n-1)$. By the previous paragraph, $\gamma^i\tau\gamma^{-i} = (i(i+1))$ and $(12)\tau(12) = (02)$ and in general $(i(i+1))(0i)(i(i+1)) = (0(i+1))$. Finally $(0j)(0i)(0j) = (ji)$ (provided $i \neq j$). Every transposition can, therefore, be written as a product of τ and γ and hence so does every element of S_n.

3. (Harder) Let $\tau = (0i)$ for $0 \leqslant i < n$ and $\gamma = (01\dots n-1)$. Find a necessary and sufficient condition on i so that τ and γ generate S_n.

   Solution: Let us prove that τ and γ generate S_n if and only if $\gcd(i,n) = 1$. Let us first assume that $\gcd(i,n) = 1$. Then i generates $\mathbb{Z}/n\mathbb{Z}$ and hence the ij for $0 \leqslant j < n$ are all distinct. Let $\sigma \in \mathfrak{S}_n$ be the permutation sending j to ij and let $f : S_n \to S_n$ be the map $x \mapsto \sigma^{-1}x\sigma$. Then f is a group homomorphism : $f(xy) = \sigma^{-1}xy\sigma = \sigma^{-1}x\sigma\sigma^{-1}y\sigma = f(x)f(y)$. Moreover f is injective as $f(x) = \sigma^{-1}x\sigma = 1$ implies $x = \sigma\sigma^{-1} = 1$ and hence f is a bijection (it is an injective function of a finite set into itself). So f is a group automorphism. Moreover $f(\tau) = (\sigma^-1(0)\sigma^{-1}(i)) = (01)$ and $f(\gamma^i)(j) = \sigma^{-1}\gamma^i\sigma(j) = \sigma^{-1}(\gamma^i(ij)) = \sigma^{-1}(i(j+1)) = j+1$. It follows that $f(\gamma^i) = \gamma$. In the previous question we showed that $f(\tau)$ and $f(\gamma^i)$ generates S_n. Because f is an automorphism, it follows that γ^i and τ generate S_n and hence so do τ and γ.

   The converse is more complicated. Let us assume that $\gcd(i,n) = d \neq 1$. The idea is to show that there is a property of γ and τ that is preserved under composition and which does not hold of all permutations. The property is the following. Let σ be either γ or τ. If $x = y \mod d$, then $\sigma(x) = \sigma(y) \mod d$. If $\sigma = \gamma$ this is obvious as $\gamma(x) = x+1$ and $d|x-y$ implies $d|(x+1)-(y+1) = x-y$. For $\sigma = \tau$ we can check all cases. If x and $y \notin \{0,i\}$, then $\tau(x) = x$ and $\tau(y) = y$ and that is obvious. If $x = 0$ and $y = i$, then $d|x-y = i$ and $d|\sigma(x)-\sigma(y) = -i$. If $x = 0$ and $y \neq i$ then if $d|x-y = -y$ we also have that $d|\sigma(x)-\sigma(y) = i-y$. The remaining cases are proved similarly.

   Let us now prove that this property is preserved under composition. If σ_1 and σ_2 are such that if $d|x-y$ then $d|\sigma_k(x)-\sigma_k(y)$ for $k = 1,2$, then if $d|x-y$, then $d|\sigma_1(x)-\sigma_1(y)$ and thus $d|\sigma_2(\sigma_1(x))-\sigma_2(\sigma_1(y))$. So if τ and γ generated S_n, it would follow that every element in S_n have this property. But $\sigma = (01)$ does not have this property as $d|i-0$ but d does not divide $\sigma(i)-\sigma(0) = i-1$ (as $d \neq 1$). Therefore γ and τ do not generate S_n.

4. Show that if Ω is an infinite set then S_Ω is infinite.

Solution: Because Ω is infinite, there are elements $a_i \in \Omega$ for all $i \in \mathbb{Z}_{\leqslant 0}$ such that $a_i = a_j$ if and only if $i = j$ (i.e. $\mathbb{Z}_{\leqslant 0}$ can be embedded in Ω). Then the transpositions $(a_0 a_i)$ for $i \in \mathbb{Z}_{>0}$ are all distinct elements of S_Ω and hence S_Ω is infinite.

5. (Harder) Assume that Ω is countable, show that S_Ω has cardinality continuum (i.e. is in bijection with 2^Ω).

   Solution: We know that S_Ω (being a subset of Ω^Ω) has cardinality at most continuum. To show that it is exactly continuum, we have to show that 2^Ω can be injected into S_Ω. Because Ω is countable, let us assume that $\Omega = \mathbb{Z}$. For every $f \in 2^{\mathbb{Z}}$, let $\sigma_f(2i) = 2i$ and $\sigma_f(2i+1) = 2i+1$ if $f(i) = 0$ and $\sigma_f(2i) = 2i+1$ and $\sigma_f(2i+1) = 2i$ otherwise. Then $\sigma_f \in S_\Omega$ and $\sigma_f = \sigma_g$ implies that $f = g$. It follows that f is an injection from 2^Ω into S_Ω.

Problem 3 :
Let G be a group whose cardinal is even.

1. Let $X = \{g \in G : g \neq g^{-1}\}$. Show that $|X|$ is even.

   Solution: The general idea is that every element $g \in X$ comes with its inverse so there must be an even number of elements in X. Let us now do an actual proof (there are many ways to see this, this is but one approach).

   Let $E \subseteq X$ be the equivalence relation xEy if $x = y^-1$ or $x = y$ (one can easily check that this is an equivalence relation). The classes of E have exactly two elements (because no element of X is its own inverse) and X is partitioned into k E-classes. If follows that $|X| = 2k$.

2. Show that there is a element of order 2 in G.

   Solution: G is the disjoint union of X and $Y = \{x \in g : x^-1 = x\}$. Because $|G|$ and X are even and $|G| = |X| + |Y|$, it follows that $|Y|$ is even. But $1 \in Y$ so Y has to contain an element $x \neq 1$ such that $x = x^{-1}$, i.e. $x^2 = 1$.

Problem 4 :
Let $(G, \cdot)$ and $(H, \star)$ be to groups. We define $(g_1, h_1) \circ (g_2, h_2) := (g_1 \cdot g_2, h_1 \star h_2)$.

1. Show that $(G \times H, \circ)$ is a group.

   Solution: First $\circ$ is indeed a map from $(G \times H)^2$ to $G \times H$. Let us now check associativity. Pick any $g_1, g_2, g_3 \in G$ and $h_1, h_2, h_3 \in H$. We have:

$$\begin{aligned}((g_1, h_1) \circ (g_2, h_2)) \circ (g_3, h_3) &= (g_1 \cdot g_2, h_1 \star h_2) \circ (g_3, h_3) \\ &= ((g_1 \cdot g_2) \cdot g_3, (h_1 \star h_2) \star h_3) \\ &= (g_1 \cdot (g_2 \cdot g_3), h_1 \star (h_2 \star h_3)) \\ &= (g_1, h_1) \circ (g_2 \cdot g_3, h_2 \star h_3) \\ &= (g_1, h_1) \circ ((g_2, h_2) \circ (g_3, h_3))\end{aligned}$$

   Let us now show that $(1_G, 1_H) \in G \times H$ is the identity. Pick $g \in G$ and $h \in H$, then $(g, h) \circ (1_G, 1_H) = (g \cdot 1_G, h \star 1_H) = (g, h) = (1_G \circ g, 1_H \star h) = (1_G, 1_H) \circ (g, h)$. Finally, let $g \in G$ and $h \in H$ and let us show that $(g^{-1}, h^{-1}) \in G \times H$ is its inverse. We have $(g, h) \circ (g^{-1}, h^{-1}) = (g \cdot g^{-1}, h \star h^{-1}) = (1_G, 1_H) = (g^{-1} \cdot g, h^{-1} \star h) = (g^{-1}, h^{-1}) \circ (g, h)$.

2. Show that $G \times H$ is Abelian if and only if G and H are.

   Solution: Assume $G \times H$ is Abelian and pick $g_1, g_2 \in G$. Then $(g_1 \cdot g_2, 1_H) = (g_1, 1_H) \circ (g_2, 1_H) = (g_2, 1_H) \circ (g_1, 1_H) = (g_2 \cdot g_1, 1_H)$.It follows that $g_1 \cdot g_2 = g_2 \cdot g_1$ and hence G is Abelian. By a symmetric argument, H is Abelian.

   Let us now assume that G and H are Abelian and pick $g_1, g_2 \in G$ and $h_1, h_2 \in H$. Then $(g_1, h_1) \circ (g_2, h_2) = (g_1 \cdot g_2, h_1 \cdot h_2) = (g_2 \cdot g_1, h_2 \cdot h_1) = (g_2, h_2) \circ (g_1, h_1)$. So $G \times H$ is Abelian.

3. (Harder) Let $(G_i)_{i \in I}$ be a collection of groups. Show that $\prod_{i \in I} G_i$ with the coordinate-wise operation, i.e. $(g_i)_{i \in I} \cdot (h_i)_{i \in I} = (g_i \cdot h_i)_{i \in I}$, is a group.

   Solution: First of all, if g_i and $h_i \in G_i$ for all i, then $(g_i \cdot h_i)_{i \in I} \in \prod_i G_i$ so the coordinate-wise operation is indeed a binary operation. Let us now prove it is associative. Pick any g_i, h_i and $t_i \in G_i$ for all i:

$$
\begin{array}{rcl}
((g_i)_{i \in I} \cdot (h_i)_{i \in I}) \cdot (t_i)_{i \in I} & = & (g_i \cdot h_i)_{i \in I} \cdot (t_i)_{i \in I} \\
& = & ((g_i \cdot h_i) \cdot t_i)_{i \in I} \\
& = & (g_i \cdot (h_i \cdot t_i))_{i \in I} \\
& = & (g_i)_{i \in I} \cdot (h_i \cdot t_i)_{i \in I} \\
& = & (g_i)_{i \in I} \cdot ((h_i)_{i \in I} \cdot (t_i)_{i \in I})
\end{array}
$$

   Let us now show that $(1_{G_i})_{i \in I}$ is the identity. Pick $g_i \in G_i$ for all i, then $(g_i)_{i \in I} \cdot (1_{G_i})_{i \in I} = (g_i \cdot 1_{G_i})_{i \in I} = (g_i)_{i \in I} = (1_{G_i} \cdot g_i)_{i \in I} = (1_{G_i})_{i \in I} \cdot (g_i)_{i \in I}$. Finally, pick $g_i \in G_i$, for all i, and let us show that $(g_i^{-1})_{i \in I}$ is its inverse. We have $(g_i)_{i \in I} \circ (g_i^{-1})_{i \in I} = (g_i \cdot g_i^{-1})_{i \in I} = (1_{G_i})_{i \in I} = (g_i^{-1} \cdot g_i)_{i \in I} = (g_i^{-1})_{i \in I} \circ (g_i)_{i \in I}$.