Corrigé (3M 270, janvier 2016)

I.1^o/ Comme le groupe $(\mathbb{Z}/9\mathbb{Z})^* = \{\bar{1},\bar{2},\bar{4},\bar{5},\bar{7},\bar{8}\}$ est d'ordre $\phi(9) = 3.2 = 6$, l'ordre de $\bar{2}$ divise 6. Comme 2^2 et $2^3 \not\equiv 1 \pmod 9$, ce n'est ni 2 ni 3 (ni 1), donc $\bar{2}$ est d'ordre 6. [Ou noter que $2^3 \equiv -1 \pmod 9$, donc $\bar{2}^3$ est d'ordre 2, donc $\bar{2}$ est d'ordre 3×2.]
2^o/ Par conséquent, le groupe $(\mathbb{Z}/9\mathbb{Z})^*$ est cylique d'ordre 6. Comme 7 est premier, $(\mathbb{Z}/7\mathbb{Z})^* = \mathbb{F}_7^*$ est aussi cyclique, et d'ordre $\phi(7) = 6$, donc $(\mathbb{Z}/9\mathbb{Z})^* \simeq \mathbb{Z}/6\mathbb{Z} \simeq (\mathbb{Z}/7\mathbb{Z})^*$.
3^o/ Par le lemme chinois (version multiplicative) et puisque $\mathbb{F}_5^*$ est cyclique d'ordre 4, $(\mathbb{Z}/N\mathbb{Z})^* \simeq (\mathbb{Z}/5\mathbb{Z})^* \times (\mathbb{Z}/7\mathbb{Z})^* \times (\mathbb{Z}/9\mathbb{Z})^* \simeq (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z})$, qui, par le lemme chinois, est isomorphe à $(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})^2 \times (\mathbb{Z}/3\mathbb{Z})^2 \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z}) \times (\mathbb{Z}/12\mathbb{Z})$. Ses facteurs invariants sont donc $\{2, 6, 12\}$.
4^o/ Dans cette décomposition, l'ordre de $x = (a, b, c)$ est le ppcm de $o(a), o(b), o(c)$, qui vaut 12 si et seulement si ou bien $o(c) = 12$, ce qui fournit $|(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z})| \times \phi(12) = 12 \times 4 = 48$ éléments, ou bien $o(c) = 4$ et $o(b) = 3$ ou 6, donnant $|(\mathbb{Z}/2\mathbb{Z})| \times (\phi(3) + \phi(6)) \times \phi(4) = 16$ éléments. Il y a donc 64 éléments x d'ordre 12.

II.1^o/ Pour $i = 1, ..., k$, soit ℓ_i la longueur du cycle c_i. Comme les c_i ont des supports disjoints, l'ordre de $c_1...c_k$ est le ppcm des ℓ_i. Ainsi chaque ℓ_i divise le nombre premier p, donc vaut p ou 1. Comme σ ne fixe aucun point, aucun des c_i n'est de longueur 1 (autrement dit : tout $j \in \{1, ..., m\}$ apparaît dans le support d'un c_i de longueur > 1). Donc $\ell_i = p$ pour tout i, et $m = \Sigma_{i=1,...,k}\ \ell_i = pk$.
2^o/ Soit g un élément d'ordre $p = 2$ de G (il en existe d'après Cauchy). Alors, la permutation $\sigma := \phi(g) \in \mathcal{S}_{2n}$ n'a aucun point fixe (car $\forall x \in G, g.x \neq x$), et est d'ordre 2 car ϕ est injective. Donc la décomposition de σ en produit de cycles disjoints ne fait intervenir que des cycles $c_1, ..., c_k$ de longueur $\ell_i = 2$, avec $2n = 2k$, c-à-d. $k = n$ transpositions. La signature de $\phi(g)$ vaut donc $(-1)^n$, qui vaut -1 puisque n est impair.
3^o/ Soit $\epsilon : \mathcal{S}_{2n} \to \{\pm 1\}$ l'homomorphisme de signature. Alors, $\epsilon \circ \phi : G \to \{\pm 1\}$ est un homomorphisme de groupes, et la question précédente montre qu'il est surjectif. Son noyau $H := Ker(\epsilon \circ \phi)$ est donc un sous-groupe de G d'indice $[G : H] = |\{\pm 1\}| = 2$.

III.1^o/ (NB : $p := 31$ est bien un nombre premier.) $n_p \equiv 1 \bmod 31$, et n_p divise 32, donc vaut 1 ou 32, donc 32 vu l'hypothèse.
2^o/ Soit $H_1, ..., H_{32}$ les p-Sylows de G. Comme p est la plus grande puissance de p divisant $|G|$, chaque H_j est d'ordre p, donc chaque élément $\neq e_G$ de H_j est d'ordre p, et engendre H_j. Deux p-Sylows $H_j, H_{j'}$ distincts ne se rencontrent donc qu'en e_G. Par ailleurs, tout élément d'ordre p de G engendre l'un des H_j. Ainsi, il y a $32 \times \phi(31) = 32 \times 30 = 960$ éléments de G d'ordre $p = 31$.
3^o/ Par Sylow, G admet au moins un 2-Sylow K, et celui-ci a $2^5 = 32$ éléments. S'il existait un second 2-Sylow K', celui-ci admettrait un élément $g' \notin K$, et d'ordre divisant 2^5, donc différent de p. D'après la question précédente, G admettrait au moins $960 + 32 + 1 > 992$ éléments. Contradiction.
4^o/ Supposons que G soit un groupe simple d'ordre 992. On vient de voir que si $n_p > 1$, il n'admet qu'un 2-Sylow K, qui est donc distingué dans G (et $\neq \{e_G\}, G$), ce que la simplicité de G interdit. Donc $n_p = 1$. Mais alors, l'unique p-Sylow H de G est distingué, contradiction.

IV.1^o/ a) $n_{11}(N)$ est $\equiv 1 \bmod 11$, et divise 3, donc vaut 1. $n_3(N)$ est $\equiv 1 \bmod 3$ et divise 11, donc vaut 1. - b) Par conséquent, l'unique 11-, resp. 3-, Sylow K, resp. H, de N est distingué dans N, et N est isomorphe au produit direct $K \times H$. Comme $K \simeq \mathbb{Z}/3\mathbb{Z}, H \simeq \mathbb{Z}/11\mathbb{Z}$, le lemme chinois entraîne que $N \simeq \mathbb{Z}/33\mathbb{Z}$.

2^o/ Soit $x \notin N$. Alors, la classe à gauche xN (resp. à droite Nx) de x modulo N est distincte, donc disjointe, de la classe N, et G est réunion disjointe de N et xN, resp. de N et de Nx. Ainsi, $xN = Nx$, et bien sûr, $yN = Ny$ pour $y \in N$. Donc $\forall g \in G, gNg^{-1} = N$.
3^o/ a) $n_{11}(G)$ est $\equiv 1$ modulo 11 et divise 6, donc vaut 1. - b) Comme l'unique 11-Sylow K de G est distingué dans G, la partie $N := KH$ de G en est un sous-groupe, d'ordre 33 puisque $K \cap H = \{e_G\}$. Il est donc cyclique, et distingué dans G car d'indice $\frac{66}{33} = 2$.
4^o/ Soient $h \in H$, qu'on peut supposer $\neq e_G$, donc d'ordre 3, et $g \in G$. Alors, h appartient au sous-groupe distingué KH de G, donc $ghg^{-1} \in KH$, et c'est un élément d'ordre 3 du groupe KH. Comme KH est cyclique, il admet un unique sous-groupe d'ordre 3, à savoir H. Donc $ghg^{-1} \in H$ pour tout $g \in G$, et $H \triangleleft G$.
5^o/ a) Comme K et H sont distingués dans G, $KH \simeq K \times H$. Soit S l'unique 2-Sylow de G. Alors S est distingué dans G, et $S \cap KH = \{e_G\}$ pour des raisons d'ordres. Donc G, d'ordre $|KH|.|S|$, est isomorphe à $KH \times S \simeq K \times H \times S$. On conclut par le lemme chinois. - b) Le groupe diédral D_{33}, d'ordre 66, n'est pas abélien, donc pas cyclique.
6^o/ a) Soit s l'élément d'ordre 2 de $\mathbb{Z}/2\mathbb{Z}$. Un tel homomorphisme ϕ est déterminé par $\phi(s) := f$, où f est un élément quelconque d'ordre divisant 2 de $Aut(\mathbb{Z}/33\mathbb{Z})$. Or $Aut(\mathbb{Z}/33\mathbb{Z}) \simeq (\mathbb{Z}/33\mathbb{Z})^* \simeq (\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/11\mathbb{Z})^* = \mathbb{F}_3^* \times \mathbb{F}_{11}^*$ et tout corps de cardinal premier $p \neq 2$ admet exactement deux racines carrées $\{1, -1\}$ de 1. Donc $Aut(\mathbb{Z}/33\mathbb{Z})$ a quatre éléments d'ordre divisant 2 : $f_1 = id$, et trois éléments f_2, f_3, f_4 d'ordre 2. Il y a donc 4 homomorphismes distincts ϕ_i de $\mathbb{Z}/2\mathbb{Z}$ dans $Aut(\mathbb{Z}/33\mathbb{Z})$, avec $\phi_i(s) = f_i$.

b) Via l'isomorphisme $Aut(\mathbb{Z}/33\mathbb{Z}) \simeq (\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/11\mathbb{Z})^*$, tout automorphisme f d'ordre divisant 2 de $\mathbb{Z}/33\mathbb{Z}$ est représenté par un couple (a, b), avec $a \equiv \pm 1 \mod 3$ et $b \equiv \pm 1 \mod 11$, et est donc représenté dans $(\mathbb{Z}/33\mathbb{Z})^*$ par la classe de $k_1 \equiv 1, k_2 \equiv -1, k_3 \equiv 10$, ou $k_4 \equiv -10$ modulo 33. Fixant un générateur r de $\mathbb{Z}/33\mathbb{Z}$, et écrivant dorénavant les lois de groupes de $\mathbb{Z}/33\mathbb{Z}$ et des G_i multiplicativement, on a alors : $f_i(r) = r^{k_i}$. Par conséquent, pour tout $i = 1, ..., 4$, le produit semi-direct $G_i =< r > \rtimes_{\phi_i} < s >$ est caractérisé par la relation $\phi_i(s)(r) = srs^{-1} = r^{k_i}$. Pour $k_1 = 1$, on reconnait ici le groupe cyclique $G_1 = \mathbb{Z}/33\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, qui a $\nu_1 = 1$ élément d'ordre 2; pour $k_2 = -1$, le groupe diédral $G_2 := D_{33} = \mathbb{Z}/33\mathbb{Z} \rtimes_{\phi_2} \mathbb{Z}/2\mathbb{Z}$, dont les symétries forment les $\nu_2 = 33$ éléments d'ordre 2. Plus généralement, les éléments d'ordre 2 de G_i ne peuvent être dans $< r >$, d'ordre impair, et sont donc de la forme sr^t, avec $t \in \mathbb{Z}/33\mathbb{Z}$ et $1 = sr^t.sr^t = sr^ts^{-1}r^t = r^{(k_i+1)t}$, soit $(k_i + 1)t \equiv 0$ modulot 33. Pour $k_1 = 1$, resp. $k_2 = -1$, on retrouve l'unique solution $t \equiv 0 \mod 33$, donc $\nu_1 = 1$, resp. les $\nu_2 = 33$ solutions $t \equiv 0, ..., 32$ modulo 33. Pour $k_3 = 10$, les solutions sont données par la condition $t \equiv 0 \mod 3$, d'où $\nu_3 = \frac{33}{3} = 11$ éléments d'ordre 2 dans G_3. Enfin, pour $k_4 = -10$, la condition $9t \equiv 0 \mod 33$ équivaut à $t \equiv 0, 11$ ou $22 \mod 33$, et il y a $\nu_4 = 3$ éléments d'ordre 2 dans G_4.
[Autre méthode : soit $i \in [1, ..., 4]$. Le groupe G_i est d'ordre 66, donc ses 2-Sylows sont d'ordre 2, et sont donc en bijection avec les éléments d'ordre 2 de G_i. Ainsi, $\nu_i = n_2(G_i)$, et si x_i désigne un élément d'ordre 2 de G_i, tous les autres forment l'orbite de x_i sous l'action de G_i sur lui-même par conjugaison. Choisissant $x_i = s = (1, s) \in < r > \rtimes_{\phi_i} < s >$, il reste à calculer le nombre de conjugués de s dans G_i. Ceux-ci sont de la forme $r^tsr^{-t}, t \in \mathbb{Z}/33\mathbb{Z}$. De $Int(r)(s) = rsr^{-1} = sr^{k_i-1}$, on tire : $Int(r^t)(s) = sr^{t(k_i-1)}$. Ainsi, ν_i est égal à l'ordre de r^{k_i-1}, soit $\nu_1 = o(r^0) = 1, \nu_2 = o(r^2) = 33, \nu_3 = o(r^9) = 11, \nu_4 = o(r^{11}) = 3$.]

c) G contient un sous-groupe distingué $N \simeq \mathbb{Z}/33\mathbb{Z}$ et un sous-groupe $S \simeq \mathbb{Z}/2\mathbb{Z}$, avec $N \cap S = \{e_G\}$ et $|N|.|S| = |G|$, donc c'est un produit semi-direct, nécessairement isomorphe à l'un des G_i. Et ces groupes G_i sont deux à deux non isomorphes puisqu'ils n'ont pas le même nombre d'éléments d'ordre 2.