

FALL 2004 PRELIMINARY EXAMINATION SOLUTIONS

1A. Show that there is a unique piecewise continuous function $y(x)$ on \mathbb{R} satisfying the two conditions

$$\begin{aligned} y(x) &= \int_0^{\infty} e^{-2s} y(x-s) ds && \text{for } x > 0, \text{ and} \\ y(x) &= e^x, && \text{for } x \leq 0, \end{aligned}$$

and find an explicit formula for $y(x)$ for $x > 0$.

Solution: Suppose that $y(x)$ is a solution. For $x > 0$, the substitution $s = x - t$ yields

$$\begin{aligned} y(x) &= \int_{-\infty}^x e^{-2(x-t)} y(t) dt \\ (1) \quad e^{2x} y(x) &= \int_{-\infty}^x e^{2t} y(t) dt. \end{aligned}$$

The right hand side is continuous as a function of x , so $e^{2x} y(x)$ is continuous on $\mathbb{R}_{>0}$, and multiplying by e^{-2x} shows that $y(x)$ is continuous on $\mathbb{R}_{>0}$. This in turn implies that the right hand side is differentiable, and the same argument now shows that $y(x)$ is differentiable on $\mathbb{R}_{>0}$. Differentiating both sides for $x > 0$ yields

$$\begin{aligned} e^{2x}(y' + 2y) &= e^{2x}y \\ y' + 2y &= y \\ y' &= -y \\ y &= ce^{-x} \end{aligned}$$

for some $c \in \mathbb{R}$. Substituting this back into (1) yields, for $x > 0$,

$$\begin{aligned} ce^x &= \int_{-\infty}^0 e^{3t} dt + \int_0^x ce^t dt \\ ce^x &= \frac{1}{3} + c(e^x - 1) \\ c &= \frac{1}{3} \\ y(x) &= \frac{1}{3}e^{-x}. \end{aligned}$$

Thus if there is a solution, it must be

$$y(x) = \begin{cases} \frac{1}{3}e^{-x} & \text{if } x > 0 \\ e^x & \text{if } x \leq 0 \end{cases}$$

Because (1) is equivalent to the integral equation in the original problem, this function indeed satisfies the conditions of the problem.

2A. For $c \in \mathbb{Q}$, define $R_c := \mathbb{Q}[x]/(x^3 - cx)$. Let $a, b \in \mathbb{Q}$. Show that the rings R_a and R_b are isomorphic if and only if there exists a nonzero $r \in \mathbb{Q}$ such that $b = r^2a$.

Solution: If $r \neq 0$ and $b = r^2a$, then the ring automorphism $\mathbb{Q}[x] \rightarrow \mathbb{Q}[x]$ sending x to rx maps $x^3 - bx$ to $r^3x^3 - brx = r^3(x^3 - ax)$, so it induces an isomorphism between the quotient rings

$$R_b = \frac{\mathbb{Q}[x]}{(x^3 - bx)} \simeq \frac{\mathbb{Q}[x]}{(r^3(x^3 - ax))} = \frac{\mathbb{Q}[x]}{(x^3 - ax)} = R_a.$$

Conversely, suppose $R_a \simeq R_b$. The maximal ideals of R_a correspond bijectively to maximal ideals of $\mathbb{Q}[x]$ containing $x^3 - ax$, which in turn correspond bijectively to distinct irreducible factors of $x^3 - ax$. Thus R_a has 1, 3, or 2 maximal ideals according as $a = 0$, a is a nonzero square, or a is not a square. Since R_b must have the same number of maximal ideals, we immediately deduce that $b = r^2a$ for some r , except possibly in the case where neither a nor b is a square. We now assume we are in this remaining case. The quotient fields of R_a (the quotients of R_a by its two maximal ideals) are \mathbb{Q} and $\mathbb{Q}[x]/(x^2 - a) \simeq \mathbb{Q}[\sqrt{a}]$. These must be the same as the quotient fields \mathbb{Q} and $\mathbb{Q}[\sqrt{b}]$ of R_b , in some order. Since b is a square in $\mathbb{Q}[\sqrt{b}]$ but not in \mathbb{Q} , it must be a square in $\mathbb{Q}[\sqrt{a}]$. Write

$$(r\sqrt{a} + s)^2 = b.$$

Expanding, we get $2rs = 0$. If $r = 0$, we contradict the assumption that b is not a square. Thus $s = 0$, and $b = r^2a$.

3A. Let f and g be functions that are holomorphic on all of \mathbb{C} , except that g has an essential singularity at the complex number c . Prove that either f is constant, or the composition $f \circ g$ has an essential singularity at c . (Hint: you may assume the Casorati-Weierstrass Theorem, which states that if a function f has an essential singularity at c , then for any punctured neighborhood N of c on which f is holomorphic, the image $f(N)$ is dense in \mathbb{C} .)

Solution: Suppose that f is not constant. Choose $a, b \in \mathbb{C}$ such that $f(a) \neq f(b)$. If N is any punctured neighborhood of c , then $g(N)$ is dense in \mathbb{C} , by the Casorati-Weierstrass Theorem. In particular, the closure of $g(N)$ contains a and b , so the closure of $f(g(N))$ contains $f(a)$ and $f(b)$. Since this holds for every N , the limit $\lim_{z \rightarrow c} f(g(z))$ is not ∞ , and does not exist as a complex number either. Thus $f \circ g$ has neither a pole nor a removable singularity at c , so it has an essential singularity at c .

4A. Let A be an $n \times n$ matrix with complex entries. Prove that A is diagonalizable if and only if the following is true: Whenever f is a polynomial with complex coefficients such that $f(A)$ is nilpotent, we have $f(A) = 0$. (A matrix A is *nilpotent* if $A^m = 0$ for some $m \geq 1$.)

Solution: First suppose that A is diagonalizable. If C is an invertible $n \times n$ matrix, then $f(CAC^{-1}) = Cf(A)C^{-1}$, so both sides of the “if and only if” are unchanged by conjugation. Thus we may assume A is diagonal. Then $f(A)$ is diagonal for any f . Hence if $f(A)$ is nilpotent, then $f(A) = 0$.

Now suppose, conversely, that A is such that $f(A) = 0$ whenever $f(A)$ is nilpotent. Let $f(x)$ be the product of $(x - \lambda)$ where λ runs through the *distinct* eigenvalues of A . Then

the characteristic polynomial $c(x)$ of A divides some power of $f(x)$, but $c(A) = 0$ (Cayley-Hamilton Theorem), so some power of $f(A)$ is 0. By hypothesis, $f(A) = 0$. Thus the minimal polynomial of A has distinct zeros, so A is diagonalizable.

5A. Let $(a_m)_{m \geq 1}$ be a sequence of real numbers satisfying $a_{n+m} \leq a_n + a_m$. Prove that

$$\lim_{n \rightarrow \infty} \frac{a_n}{n} = \inf_n \frac{a_n}{n}$$

as an element of $[-\infty, \infty)$.

Solution: If $n = \ell m + r$ for integers $m, \ell \geq 1$ and $r \in [0, m)$, then $a_n = a_{\ell m + r} \leq \ell a_m + a_r \leq \ell a_m + a_r$, and dividing by n yields

$$\frac{a_n}{n} \leq \frac{\ell m}{n} \frac{a_m}{m} + \frac{a_r}{n}.$$

After sending $n \rightarrow \infty$ (for fixed m , so ℓ and r vary with n), we obtain

$$\limsup \frac{a_n}{n} \leq \frac{a_m}{m}.$$

This holds for each m , so

$$\limsup \frac{a_n}{n} \leq \inf \frac{a_m}{m}.$$

On the other hand,

$$\liminf \frac{a_n}{n} \geq \inf \frac{a_m}{m}$$

holds by definition. Thus

$$\lim \frac{a_n}{n} = \inf \frac{a_m}{m}.$$

6A. Let n be a square-free positive integer (*i.e.*, $n = 1$ or n is prime or n is a product of distinct primes). Assume that for every product of primes $p q_1 \cdots q_r$ dividing n , with $r > 0$, we have $q_1 \cdots q_r \not\equiv 1 \pmod{p}$. Prove that every group G of order n is abelian.

Solution: Suppose $p|n$ and let P be a Sylow p -subgroup of G . Let N be the normalizer of P . By Sylow's theorems, the number of Sylow p -subgroups is $[G : N] \equiv 1 \pmod{p}$. Since N contains P , we have $[G : N] = q_1 \cdots q_r$, where $p q_1 \cdots q_r | n$. Our hypothesis implies that $r = 0$, hence $N = G$, so P is normal. Now let $n = p_1 \cdots p_k$ and let P_1, \dots, P_k be the corresponding normal Sylow subgroups. Let $Q_i \subseteq G$ be the product of the P_j 's, omitting P_i . Then Q_i is normal and G/Q_i is cyclic of order p_i . Thus we have a surjective homomorphism $\phi_i: G \rightarrow \mathbb{Z}/p_i\mathbb{Z}$ for each i , and combining these, we get a homomorphism $\phi: G \rightarrow \prod_i \mathbb{Z}/p_i\mathbb{Z}$. Let $K = \ker(\phi)$. Since each ϕ_i factors through G/K , every p_i divides $|G/K|$. This implies $K = 0$. Then ϕ is an injective homomorphism between two groups of equal order, hence an isomorphism.

7A. Let D be the open unit disk in \mathbb{C} , and $f: D \rightarrow D$ a holomorphic function. Suppose that $f(-\frac{1}{2}) = 0$ and $f(0) = \frac{1}{2}$. Prove that there is only one possible value for $f(\frac{1}{2})$, and find it.

Solution: We first solve for a linear fractional transformation g of D mapping

$$g\left(-\frac{1}{2}\right) = 0, \quad g(0) = \frac{1}{2}$$

and find that the function

$$g(z) = \frac{z + \frac{1}{2}}{1 + \frac{z}{2}} = \frac{2z + 1}{2 + z}$$

satisfies these conditions. Then the composition $h = f \circ g^{-1}$ satisfies

$$h: D \rightarrow D, \quad h(0) = 0, \quad h\left(\frac{1}{2}\right) = \frac{1}{2}$$

By Schwarz's lemma we must have $|h(z)| \leq |z|$ in D . But equality holds for $z = \frac{1}{2}$, so $h(z)$ must equal z . Hence $f = g$, and

$$f\left(\frac{1}{2}\right) = \frac{4}{5}.$$

8A. Let $\langle \cdot, \cdot \rangle$ be a positive-definite Hermitian inner product on a finite-dimensional complex vector space V . Suppose $T: V \rightarrow V$ is a \mathbb{C} -linear map such that $\langle Tv, v \rangle = 0$ for all $v \in V$. Prove that $T = 0$.

Solution: For $x, y \in V$, expanding

$$\langle T(x + y), (x + y) \rangle - \langle Tx, x \rangle - \langle Ty, y \rangle = 0$$

yields

$$\langle Tx, y \rangle + \langle Ty, x \rangle = 0.$$

Substituting ix for x yields

$$i\langle Tx, y \rangle - i\langle Ty, x \rangle = 0.$$

The previous two equalities imply $\langle Tx, y \rangle = 0$ for all $x, y \in V$. Taking $y = Tx$, we get $\langle Tx, Tx \rangle = 0$. Since $\langle \cdot, \cdot \rangle$ is positive-definite, we get $Tx = 0$. This holds for all $x \in V$, so $T = 0$.

Remark: this proof works even when V is infinite-dimensional.

9A. Let $f: [0, 1] \rightarrow \mathbb{R}$ be a continuous function. Show that

$$\lim_{n \rightarrow \infty} \int_0^1 f(x) e^{inx^3} dx = 0.$$

Solution: We can approximate f uniformly by smooth functions in $[0, 1]$, so it suffices to prove the statement when f is smooth.

Choose M such that $|f(x)| < M$ for all $x \in [0, 1]$. Let $\epsilon > 0$. Then

$$\left| \int_0^\epsilon f(x) e^{inx^3} dx \right| \leq \epsilon M$$

On the remaining interval we integrate by parts:

$$\begin{aligned} \int_\epsilon^1 f(x) e^{inx^3} dx &= \int_\epsilon^1 \frac{f(x)}{x^2} x^2 e^{inx^3} dx \\ &= \frac{1}{in} \left(f(1) e^{in} - \frac{f(\epsilon)}{\epsilon^2} e^{in\epsilon^3} - \int_\epsilon^1 \frac{d}{dx} \left(\frac{f(x)}{x^2} \right) e^{inx^3} dx \right) \end{aligned}$$

Letting n tend to infinity, we obtain

$$\lim_{n \rightarrow \infty} \int_{\epsilon}^1 f(x) e^{inx^3} dx = 0$$

Adding to this the bound on $[0, \epsilon]$, we get

$$\limsup_{n \rightarrow \infty} \left| \int_0^1 f(x) e^{inx^3} dx \right| \leq \epsilon M$$

The conclusion follows if we let ϵ tend to 0.

1B. Let S_n be the group of permutations of $\{1, \dots, n\}$, and let A_n be the alternating subgroup. Suppose $m \leq n$.

(a) Identify S_m with the subgroup of S_n consisting of elements that fix $m+1, \dots, n$. Prove that $A_n \cap S_m = A_m$.

(b) Is it true in general that if $f: S_m \rightarrow S_n$ is an injective homomorphism, then $A_n \cap f(S_m) = f(A_m)$? Give a proof or a counterexample.

Solution: (a) By definition A_n is the kernel of the unique homomorphism $\text{sgn}_n: S_n \rightarrow \{\pm 1\}$ mapping each transposition to -1 . Restricting sgn_n to S_m gives a homomorphism mapping each transposition in S_m to -1 , so this restriction must equal sgn_m . Thus $A_m = \ker(\text{sgn}_m) = \ker(\text{sgn}_n) \cap S_m = A_n \cap S_m$.

(b) It is false. Take $m \geq 2$ and $n = 2m$. There is an obvious action of $S_m \times S_m$ on $\{1, \dots, 2m\}$ in which the first S_m permutes $\{1, \dots, m\}$ and the second S_m permutes $\{m+1, \dots, 2m\}$. Thus we get an injective homomorphism $\iota: S_m \times S_m \rightarrow S_{2m}$. Define $f: S_m \rightarrow S_{2m}$ by $f(\sigma) = \iota(\sigma, \sigma)$. Then f maps each transposition in S_m to an element of A_{2m} , and the transpositions generate S_m , so $f(S_m) \subseteq A_{2m}$. Hence $A_{2m} \cap f(S_m) = f(S_m)$, and this is strictly larger than $f(A_m)$, since f is injective.

2B. Let $f: \mathbb{R}^3 \rightarrow \mathbb{R}$ be a continuous function of compact support (i.e., f vanishes outside some bounded set).

(a) Show that

$$u(x) := \int \frac{f(y)}{|x-y|} dy$$

converges, where the integral is over all $y \in \mathbb{R}^3$.

(b) Show that $\lim_{|x| \rightarrow \infty} u(x)|x|$ exists.

Solution: (a) Let M be the maximum value of $|f|$ (this exists, since f is 0 outside some compact set and is continuous). Fix x . Choose R large enough that $f(y) = 0$ if $|x-y| > R$. Using polar coordinates centered at x , we have

$$\int \frac{|f(y)|}{|x-y|} dy \leq \int_0^R \frac{M}{r} (4\pi r^2 dr),$$

which converges, so the integral defining $u(x)$ converges absolutely.

(b) By writing $f(y) = \max\{f(y), 0\} + \min\{f(y), 0\}$, we may reduce to the case that f is nonnegative everywhere. Let $R_0 > 0$ be such that $f(y) = 0$ for $|y| > R_0$. If $|x| \geq nR_0$ where n is large, and $|y| \leq R_0$, then

$$\frac{|x|}{|x-y|} \leq \frac{|x|}{|x|-|y|} = \frac{1}{1-|y|/|x|} \leq \frac{1}{1-1/n} = \frac{n}{n-1}$$

$$\frac{|x|}{|x-y|} \geq \frac{|x|}{|x|+|y|} = \frac{1}{1+|y|/|x|} \leq \frac{1}{1+1/n} = \frac{n}{n+1}.$$

Hence

$$\frac{n}{n+1} \int f \, dy \leq u(x)|x| \leq \frac{n}{n-1} \int f \, dy$$

for large x . Thus $\lim_{|x| \rightarrow \infty} u(x)|x| = \int f \, dy$.

3B. For which positive integers n does there exist an $n \times n$ matrix A with rational entries such that $A^3 + A + I = 0$?

Solution: The polynomial $f(x) = x^3 + x + 1$ is irreducible over \mathbb{Q} (because it is irreducible modulo 2, or because of the rational root test, for instance). Since all eigenvalues of A are roots of $f(x)$, the characteristic polynomial of A divides a power of $f(x)$, and hence is equal to a power of $f(x)$ by irreducibility. Therefore n must be a multiple of 3.

Conversely, if $n = 3$, we may let $V = \mathbb{Q}[x]/(x^3 + x + 1)$, and let A be the matrix (with respect to some basis) of the \mathbb{Q} -linear transformation $V \rightarrow V$ given by multiplication by the image of x . And for n any larger multiple of 3, we can take A to be block-diagonal with each 3×3 diagonal block equal to the solution for $n = 3$.

4B. Evaluate $I(w) := \int_0^\infty \frac{e^{iwt}}{\sqrt{t}} \, dt$ for every nonzero real number w . You may use the formula

$$\int_{-\infty}^\infty e^{-x^2} \, dx = \sqrt{\pi}.$$

The substitution $t = u^2$ yields

$$I(w) = 2 \int_0^\infty f(u) \, du.$$

where $f(u) := e^{iwu^2}$. Suppose $w > 0$. For $R > 0$, let γ_1 be the straight-line path from 0 to R , let γ_2 be the circular arc Re^{it} for $t \in [0, \pi/4]$, and let γ_3 be the straight-line path from $Re^{i\pi/4}$ to 0. By Cauchy's Theorem, $\sum_{j=1}^3 \int_{\gamma_j} f(u) \, du = 0$. For $u = Re^{it}$, we have

$$|f(u)| = e^{\operatorname{Re}(iwu^2)} = e^{-w\operatorname{Im}(u^2)} = e^{-wR^2 \sin(2t)} \leq e^{-wR^2(2(2t)/\pi)},$$

where the last step comes from the inequality $\sin x \leq 2x/\pi$ for $x \in [0, \pi/2]$ (concavity of $\sin x$ on this interval). Therefore

$$\left| \int_{\gamma_2} f(u) \, du \right| \leq \int_0^\infty e^{-wR^2(2(2t)/\pi)} \, dt = \frac{\pi}{4wR^2},$$

which goes to 0 as $R \rightarrow \infty$. Hence

$$\begin{aligned}
 I(w) &= 2 \lim_{R \rightarrow \infty} \int_{\gamma_1} f(u) du \\
 &= -2 \lim_{R \rightarrow \infty} \int_{\gamma_3} f(u) du \\
 &= 2 \int_0^\infty f(e^{i\pi/4}t) e^{i\pi/4} dt \\
 &= 2 \int_0^\infty e^{-wt^2} e^{i\pi/4} dt \\
 &= e^{i\pi/4} \int_{-\infty}^\infty e^{-wt^2} dt \\
 &= e^{i\pi/4} \int_{-\infty}^\infty e^{-v^2} dv \\
 &= \frac{1+i}{\sqrt{2}} \int_{-\infty}^\infty e^{-v^2} \frac{dv}{\sqrt{w}} \\
 &= (1+i) \sqrt{\frac{\pi}{2w}}.
 \end{aligned}$$

Also, $I(-w)$ is the complex conjugate of $I(w)$. Therefore, for any $w \neq 0$,

$$I(w) = (1 + i \operatorname{sgn}(w)) \sqrt{\frac{\pi}{2|w|}}.$$

5B. What is the cardinality of the smallest field F of characteristic 7 such that the equation $x^{18} + x^{17} + \dots + x + 1 = 0$ has a solution $x \in F$?

Solution: We have the identity

$$(x-1)(x^{18} + x^{17} + \dots + x + 1) = x^{19} - 1,$$

and the latter has no repeated factors over a field of characteristic 7 (since $x^{19} - 1$ has no factors in common with its derivative), so the given condition is equivalent to the condition that the multiplicative group F^* contain a nontrivial element of order dividing 19. Since 19 is prime and F^* is a finite abelian group, this is equivalent to $19 \mid \#F^*$. The size of F is 7^m for some $m \geq 1$, so the condition becomes $19 \mid (7^m - 1)$. We compute $7^2 \equiv 11 \pmod{19}$ and $7^3 \equiv 1 \pmod{19}$, so the smallest possible m is 3, and the smallest possible field F satisfying the conditions is the field \mathbb{F}_{7^3} of $7^3 = 343$ elements.

6B. Suppose that $f(z)$ is holomorphic on all of \mathbb{C} except for a pole at $z = 0$. Prove that

$$\lim_{n \rightarrow \infty} \frac{1}{n} \sum_{k=1}^n f\left(\frac{1}{n} e^{2\pi i k/n}\right)$$

exists.

Solution: If f were holomorphic at 0, then each term in the sum would be $f(0) + O(1/n)$ where the implied constant is independent of k and n , so the average of these f -values would also be $f(0) + O(1/n)$, which tends to $f(0)$ as $n \rightarrow \infty$.

In general, using the Laurent series of f , we may write f as a finite linear combination of functions of the form z^{-m} for $m > 0$ plus one function that is holomorphic at 0. By linearity, it remains to prove the statement for $f(z) = z^{-m}$. In this case, the sum in the problem is a finite geometric series, and its value is 0 when $n > m$.

7B. Let $n \geq 1$, and let $M_n(\mathbb{R})$ be the ring of $n \times n$ matrices over the field of real numbers. What is the dimension of the subspace V of $M_n(\mathbb{R})$ spanned by the matrices of the form $AB - BA$ where $A, B \in M_n(\mathbb{R})$?

Solution: Let E_{ij} be the matrix with 1 in the (i, j) position and zeros elsewhere. Since $AB - BA$ is linear in each of A and B , the subspace V equals the span of $AB - BA$ where A is some E_{ij} and B is some $E_{k\ell}$. We have

$$E_{ij}E_{k\ell} - E_{k\ell}E_{ij} = \begin{cases} 0 & \text{if } j \neq k \text{ and } i \neq \ell \\ E_{i\ell} & \text{if } j = k \text{ and } i \neq \ell \\ -E_{kj} & \text{if } j \neq k \text{ and } i = \ell \\ E_{ii} - E_{jj} & \text{if } j = k \text{ and } i = \ell. \end{cases}$$

Varying i, j, k, ℓ , we find that V is spanned by the set of all E_{ij} with $i \neq j$ together with the set of $E_{ii} - E_{i+1, i+1}$ for $i = 1, \dots, n-1$. These matrices are clearly independent, so $\dim V = (n^2 - n) + (n-1) = n^2 - 1$. (A more elegant way to describe V is as the space of trace-zero matrices.)

8B. A C^2 function $y(x)$ for $0 \leq x \leq 1$, a positive continuous function $a(x)$ for $0 \leq x \leq 1$, and a real number λ satisfy

$$\begin{aligned} y''(x) + \lambda a(x)y(x) &= 0, \\ y(0) &= 0, \\ y'(1) &= 0. \end{aligned}$$

Suppose that $y(x)$ is not identically zero. Prove that $\lambda > 0$.

Solution: Multiply the ODE by $y(x)$ and integrate from 0 to 1 to get

$$\begin{aligned} \lambda \int_0^1 ay^2 dx &= - \int_0^1 yy'' dx \\ &= -yy'|_0^1 + \int_0^1 y'^2 dx \quad (\text{integration by parts, with } u = y, dv = y'' dx) \\ &= \int_0^1 y'^2 dx \\ &> 0, \end{aligned}$$

since if y' were identically zero on $[0, 1]$, then y would be constant on $[0, 1]$, making y identically zero (since $y(0) = 0$). Since $a > 0$ and y is not identically zero, we also have $\int_0^1 ay^2 dx > 0$. Thus λ is a ratio of positive numbers, so $\lambda > 0$.

9B. Prove that every group of order 30 has a cyclic subgroup of order 15.

Solution: Let G be the group. For primes $p|30$, let n_p be the number of Sylow p -subgroups of G . Then $n_p \equiv 1 \pmod{p}$ and $n_p|30/p$. In particular n_3 is 1 or 10, and n_5 is 1 or 6. There are $(p-1)n_p$ elements of exact order p in G . If $n_3 = 10$ and $n_5 = 6$, then $(3-1)n_3 + (5-1)n_5 > \#G$, so either $n_3 = 1$ or $n_5 = 1$.

Suppose $n_3 = 1$. Then there is a unique Sylow 3-subgroup P , and it is normal. Let g be an element of order 5 in G . Conjugation-by- g restricts to an automorphism of P of order dividing 5, but $\#\text{Aut}P = \#(\mathbb{Z}/3\mathbb{Z})^* = 2$, so this automorphism must be trivial. Thus g commutes with every element of P . Hence the group generated by g and P is isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/15\mathbb{Z}$.

If instead $n_5 = 1$, the same argument with 3 and 5 reversed works, since 3 does not divide $\#(\mathbb{Z}/5\mathbb{Z})^*$.