PROBLEM SET - CHARACTER THEORY OF FINITE GROUPS

DO HOANG VIET[1,2], TRAN MINH NGUYEN[1,2], AND NGUYEN TRUNG NGHIA[1,2]

Let A be a finite-dimensional $\mathbb{F}$-algebra.

1.1. Let U be an A-module. Show that the following statements are equivalent:

(a) U is completely reducible;
(b) every submodule of U is completely reducible;
(c) every homomorphic image of U is completely reducible.

Solution. (a) $\Rightarrow$ (b): Assume that U is completely reducible. Let $W \leq V$ be submodules of U. Since U is completely reducible, there exists a submodule W' of U such that

$$U = W \oplus W'.$$

Let $\varphi : U \to U$ be the projection map of U onto W'. Then φ is an A-homomorphism from U to itself. We will prove that $\varphi(V)$ is a submodule of V and moreover,

$$V = W \oplus \varphi(V), \tag{1}$$

from which assertion (b) follows. Indeed, we have that

$$\text{for each } v \in V,\ v = v - \varphi(v) + \varphi(v) \text{ with } v - \varphi(v) \in W \subset V \text{ and } \varphi(v) \in W', \tag{2}$$

so $\varphi(v) = v - (v - \varphi(v)) \in V$ and $\varphi(V) \subset V$. In addition, $\varphi(V)$ is a subspace of U because V is a subspace of U and φ is $\mathbb{F}$-linear; and $\varphi(V)$ is A-invariant as $\varphi(v)a = \varphi(va) \in \varphi(V)$ for all $v \in V$ and $a \in A$. We have just shown that $\varphi(V)$ is a submodule of V. Then, equation (1) holds because of (2) and the fact that $W \cap \varphi(V) \subset W \cap W' = \{0\}$. Therefore, V is completely reducible, which means every submodule of U is completely reducible.

Second approach: Let $W \leq V \leq U$ be submodules of U. We therefore have a decomposition U as a direct sum of W and some submodule W' of U, that is, $U = W \oplus W'$. The decomposition of U then defines a projection $\pi_W : U \to U$ of U onto W, that is $\pi_W^2 = \pi_W$. Define $\pi_W^* : V \to V$ determined by $\pi_W^*(v) = \pi_W(v)$ for each $v \in V$. It is clear that π_W^* is a projection of V onto W, and hence yields a decomposition of V as a direct sum of W and some W''.

Third approach: Let V be an arbitrary nonzero submodule of U. By [Isa94, Theorem 1.10], it remains to show that V is a sum of some of its irreducible submodules. Using again [Isa94, Theorem 1.10], U can be written as sum of irreducible submodules, that is $U = \sum_{i\in I} U_i$ where U_i's are irreducible submodules of U for some index set I. For each nonzero element $v \in V \subseteq U$, there is some index i such that $v \in U_i$, and therefore $0 \neq U_i \cap V \subseteq U_i$ which implies that $U_i \cap V = U_i$ since U_i is irreducible. In other words, U_i is contained in V. By taking the sum of those U_i's, we obtain that $V = \sum_{i\in J} U_i$, and henceforth is completely reducible.

(b) $\Rightarrow$ (c): Let $\varphi : U \to X$ be an arbitrary homomorphism of A-modules. Since U is completely reducible, there exists some A-submodule V of U such that $U = \ker\varphi \oplus V$. By First Isomorphism Theorem, we obtain that

$$\mathrm{im}\varphi \simeq U/\ker\varphi = (\ker\varphi \oplus V)/\ker\varphi \simeq V,$$

is completely reducible.

(c) $\Rightarrow$ (a): It is obvious since $U = \mathrm{im}(\mathrm{id}_U)$. $\square$

1.2. Let V be an A-module. Prove that V is completely reducible iff the intersection of all maximal submodules of V is 0.

Solution. Suppose that V is completely reducible. Write $V = \bigoplus_{i=1}^n V_i$ as direct sum of a finite number, due to its finite-dimensionality, of irreducible submodules (see [Isa94, Theorem 1.10 and Lemma 1.11]). By setting $M_j = \bigoplus_{i\neq j} V_i$ as maximal submodules of V, we get that $\bigcap_{\text{maximal}} M \subseteq \bigcap_{i=1}^n M_i = 0$, or $\bigcap_{\text{maximal}} M = 0$.

Conversely, suppose that the intersection of all maximal submodules of V is 0. We will show that there are finitely maximal modules whose intersection is trivial. Indeed, consider the collection of all submodules of the form $\{\bigcap_{\text{finite}} M : M \text{ is maximal}\}$. Then, since V is finite-dimensional, there is a minimal element in the collection, namely $\bigcap_{i=1}^n M_i$. If it is not identically zero, pick $0 \neq x \in \bigcap_{i=1}^n M_i$, and since $\bigcap_{\text{maximal}} M = 0$, there must be some maximal submodule M not containing x. But now $M \cap \bigcap_{i=1}^n M_i$ is proper submodule of $\bigcap_{i=1}^n M_i$, which contradicts to the fact that $\bigcap_{i=1}^n M_i$ is minimal. Thus, $\bigcap_{i=1}^n M_i = 0$. Now, the natural homomorphism of modules

$$\begin{array}{rcl} \psi : V & \to & \bigoplus_{i=1}^n V/M_i, \\ v & \mapsto & (v + M_i)_{i=1}^n, \end{array}$$

is indeed an embedding because of the identity $\bigcap_{i=1}^n M_i = 0$. It means that V is isomorphic to a submodule of a direct sum of irreducible modules, and hence completely reducible due to [Isa94, Theorem 1.10] and Exercise 1.1. □

1.3. A is semisimple iff every A-module is completely reducible.

Solution. The "if" part is straightforward since A is an A-module.

For the "only if" part, observe that from assertions (b) and (c) in Exercise 1.1, every submodule and quotient module of a completely reducible module is also completely reducible. Now let V be an A-module. For each nonzero element v of V, we get the natural isomorphism $vA \simeq A/\text{ann}(v)$. The latter module is completely reducible since it has the form of a quotient module of the regular module A°. By writing V as the sum of modules vA, that is $V = \sum_{v\in V} vA$, we conclude that V is completely reducible (see [Isa94, Theorem 1.10]).

Wrong solution for the "only if" part: Let V be an A-module. A well-known result states that every A-module is isomorphic to a quotient module of a free module, that implies $V \simeq \left(\bigoplus_{i\in I} A\right)/W$ for some submodule W and some index set I. Since the direct sum of completely reducible modules is again completely reducible, $\bigoplus_{i\in I} A$ itself is completely reducible, and hence so is $\left(\bigoplus_{i\in I} A\right)/W$ as the remark above.
Remark: There is a fundamental flaw in the solution above, that is $\bigoplus_{i\in I} A$ itself need not be a finite-dimensional space over $\mathbb{F}$. However, if we extend our definition of module over algebra to be not necessarily finite-dimensional, the above results still hold. □

1.4. Let G be a finite group and p a prime dividing $|G|$. Let $\mathbb{F}$ be a field of characteristic of p. Prove that $\mathbb{F}G$ is not semisimple.

Solution. We start by assuming the opposite, that $(\mathbb{F}G)^\circ$ is completely reducible. Put $a = \sum_{g\in G} g$. An easy computation that

$$ha = h\sum_{g\in G} g = \sum_{g\in G} hg = \sum_{g\in G} g = a = \sum_{g\in G} gh = \left(\sum_{g\in G} g\right) h = ah,$$

for each element $h \in G$ gives us that $ax = xa$ for all $x \in \mathbb{F}G$, or equivalently that $a \in Z(\mathbb{F}G)$. It is routine to check that the map

$$\begin{array}{rcl} \phi : \mathbb{F}G & \to & \mathbb{F}, \\ \sum_{g\in G} a_g g & \mapsto & \sum_{g\in G} a_g, \end{array}$$

is a well-defined nonzero $\mathbb{F}$-homomorphism of $\mathbb{F}$-algebras. We now claim that $xa(= ax) = \phi(x)a$ for all $x \in \mathbb{F}G$. Indeed, we have as follows

$$\left(\sum_{g\in G} a_g g\right) a = \sum_{g\in G} a_g g a = \sum_{g\in G} a_g a = \left(\sum_{g\in G} a_g\right) a,$$

for all $\sum_{g\in G} a_g g \in \mathbb{F}G$. Consider the $\mathbb{F}G$-module U generated by the element $a = \sum_{g\in G} g$. By the assumption of $\mathbb{F}G$ being semisimple, there exists an $\mathbb{F}G$-submodule V such that $\mathbb{F}G = U \oplus V$. Notice that $U = \mathbb{F}Ga = \mathbb{F}a$ as above. For any element v of V, we have that $va \in U \cap V = 0$, so that $va = 0$. Using the claim above, we get that $0 = va = \phi(v)a$, which implies that $\phi(v) = 0$. On the other hand, $\phi(ka) = p \times \frac{|G|}{p} k = 0$ for all $k \in \mathbb{F}$, and hence $\phi(u) = 0$ for all $u \in U$. Thus, ϕ must be identically zero on $U \oplus V = \mathbb{F}G$, a contradiction! The proof is complete.

Second approach: We use the same notations of ϕ, and remarks related to a are yet applicable. By Exercise 1.2, it suffices to show that $a = \sum_{g\in G} g \in I$ for all maximal right ideal I of $\mathbb{F}G$. Assume that there exists a maximal right ideal I of $\mathbb{F}G$ such that $a \notin I$. As the maximality of I, we have $I + a\mathbb{F}G = \mathbb{F}G$, which implies that $1 = i + ax$ for some $i \in I$ and $x \in \mathbb{F}G$. Thus, the relation $a = ia + axa = ia + a^2x = ia + \phi(a)ax = ia \in I$ contradicts to the maximality of I. $\square$

2.1. (a) Let Φ be an irreducible $\mathbb{F}$-representation of a finite group G over an arbitrary field $\mathbb{F}$. Show that $\sum_{g\in G} \Phi(g) = 0$, unless Φ is the principal representation.

(b) Let H be a subgroup of G and $g \in G$ be such that all elements of the coset Hg are G-conjugate. Let $\chi \in \mathrm{Irr}(G)$ be such that $\left(\chi\big|_H, 1_H\right)_H = 0$. Show that $\chi(g) = 0$.

Solution. (a) Suppose that $\sum_{g\in G} \Phi(g) \neq 0$. Let V be the $\mathbb{F}G$-module corresponding to the representation Φ, that is, V is determined by $vg = v\Phi(g)$ for all $v \in V$ and $g \in G$. Because $\sum_{g\in G} \Phi(g) \neq 0$, there exists a nonzero element $v \in V$ such that $v\sum_{g\in G} \Phi(g) \neq 0$. Since Φ is irreducible, so is V. As the irreducibility of V, we have that $V = v\mathbb{F}G$. Set $u = v\sum_{g\in G} g \neq 0$. It is routine that $ug = u$ for all element $g \in G$, or that $u\mathbb{F}G = u\mathbb{F}$. The irreducibility of V again shows that $V = u\mathbb{F}G = u\mathbb{F} = \mathbb{F}u$. Those facts above give us that Φ is similar to the principal representation (corresponding to the basis $\{u\}$), and hence coincides the principal representation.

(b) Notice that $|H|$ is invertible in $\mathbb{F}$ by the definition of the inner product. Let Φ be the representation affording χ. Because $\left(\chi\big|_H, 1_H\right)_H = 0$, we deduce that there is no constituent of Φ similar to the principal representation. According to part (a), $\sum_{t\in H} \Phi(t) = 0$, so $\sum_{tg\in Hg} \Phi(tg) = \sum_{tg\in Hg} \Phi(t)\Phi(g) = \left(\sum_{t\in H} \Phi(t)\right)\Phi(g) = 0$. Taking the trace at two sides of the equation, it follows that $\sum_{t\in H} \chi(tg) = 0$. Additionally, $\chi(tg) = \chi(g)$ as all elements of the coset Hg are G-conjugate. Therefore, $0 = \sum_{t\in H} \chi(tg) = |H|\chi(g) = 0$. We conclude that $\chi(g) = 0$.

$\square$

From now on, all characters are $\mathbb{C}$-characters.

2.2. Let χ be a character of G. Choose a representation Φ affording χ and define $\det\chi : G \to \mathbb{C}$ as follows: $(\det\chi)(g) = \det(\Phi(g))$. Show that $\det\chi$ does not depend on the choice of Φ, and it is a linear character of G.

Solution. Firstly, suppose that $\mathfrak{X}$ is another representation of G affording χ. As Φ and $\mathfrak{X}$ affords the same character, they are similar, i.e. there exists a nonsingular matrix T satisfying $\Phi(g) = T^{-1}\mathfrak{X}(g)T$ for all $g \in G$. As a result, $\det(\Phi(g)) = \det(T^{-1}\mathfrak{X}(g)T) = \det(\mathfrak{X}(g))$, which asserts that $\det\chi$ does not depend on the choice of the representation Φ. Secondly, we have a simple observation that $(\det\chi)(g) \in \mathbb{C}^*$ for all $g \in G$, since $\Phi(g)$ is nonsingular. Now consider the map $\rho : G \to \mathbb{C}^*$

that maps each $g \in G$ to the corresponding value $(\det \chi)(g)$. The map ρ turns out to be a linear representation because

$$\rho(g_1g_2) = (\det \chi)(g_1g_2) = \det(\Phi(g_1g_2)) = \det(\Phi(g_1)\Phi(g_2)) = \det(\Phi(g_1)) \cdot \det(\Phi(g_2)) = \rho(g_1) \cdot \rho(g_2).$$

In conclusion, $\det \chi$ is a linear character afforded by ρ. $\square$

2.3. (a) Let G be a non-abelian group of order 8. Show that G has exactly four linear characters and one more irreducible character, say χ, which is of degree 2. Show that $\chi(g) = -2$ if $g \in Z(G)$ and $g \neq 1$, and $\chi(g) = 0$ if $g \in G \setminus Z(G)$.

(b) If G is the dihedral group D_8 of order 8:

$$G = \langle a, b : a^4 = b^2 = 1, bab = a^{-1} \rangle,$$

then $\det \chi \neq 1_G$. If G is the quaternion group Q_8 of order 8:

$$G = \langle a, b : a^2 = b^2, a^4 = 1, bab^{-1} = a^{-1} \rangle,$$

then $\det \chi = 1_G$. On the other hand, observe that D_8 and Q_8 have the same character table.

Solution. Firstly, we need the following lemma:

Lemma 1. *Let G be a p-group where p is a prime. If $1 \neq N \trianglelefteq G$. Then $N \cap Z(G) \neq 1$.*

Proof of Lemma 1. We consider the action of G on N that is defined by:

$$\begin{array}{ccc} G \times N & \rightarrow & N, \\ (g, n) & \longmapsto & g^{-1}ng. \end{array}$$

As the normality of N, the above action is well-defined. We have $N = \bigsqcup_{i=1}^n \Omega_i$, where each $\Omega_i = \{g^{-1}n_ig : g \in G\}$ for some element n_i of N is an orbit of the action, so that $|N| = \sum_i |\Omega_i|$. By Orbit-stabilizer Theorem, we have

$$|N| = |N \cap Z(G)| + \sum_{n_i \notin N \cap Z(G)} |\Omega_i| = |N \cap Z(G)| + \sum_{n_i \notin N \cap Z(G)} [G : C_G(n_i)].$$

Note that $|N|$ is a power of p since it divides $|G|$, and moreover, $p \mid |N|$ as N is nontrivial. Using the analogous argument for $|\Omega_i|$ instead of $|N|$, we get that $p \mid |\Omega_i| = [G : C_G(n_i)]$ for every $n_i \notin N \cap Z(G)$. As a result, we have $p \mid |N \cap Z(G)|$, which leads to the fact that there is a nontrivial element in $N \cap Z(G)$ since $N \cap Z(G)$ containing 1 is nonempty. $\square$

Now, we split the required assertions into smaller parts:

Step 1 Prove that $Z(G) = G' \simeq \mathbb{Z}_2$:

Since G is a 2-group, the center $Z(G)$ cannot be trivial (see [Rot02, Theorem 2.103]) and moreover, $Z(G)$ is properly contained in G as G is non-abelian. Therefore, $|Z(G)| \in \{2, 4\}$. Nonetheless, if $|Z(G)| = 4$, the quotient $G/Z(G)$ is a cyclic group of order 2, say $G/Z(G) = \langle gZ(G) \rangle$. Thus, G consists of all elements g^iz where $i \in \{0, 1\}, z \in Z(G)$, which is an abelian group. A contradiction! Hence, $Z(G) \simeq \mathbb{Z}_2$.

Because G is a non-abelian, G' is a non-trivial (normal) subgroup of G. According to Lemma 1, $G' \cap Z(G)$ is nontrivial, which implies that $Z(G) \subseteq G'$. Then $G/Z(G)$ is a group of order 4, and hence is abelian, so $(G/Z(G))' = \overline{1}$. On the other hand, $G'Z(G)/Z(G) = (G/Z(G))'$. Combining two facts above, we conclude that $G' \subseteq Z(G)$, and hence $G' = Z(G)$ as desired.

Step 2 Show the existence of χ:

The fundamental formula in representation theory, that the sum of squares of degree of irreducible representations is equal to 8, shows that the degree of those characters must not exceed 2. Since G is nonabelian, there exists some χ having degree other than 1, and hence its degree is equal to 2. Besides, the existence of the principal character of G yields to the singleness of the character of order 2. As a result, there are precisely four linear characters, namely $\{\chi_i\}_{i=1}^4$, and the only one irreducible character χ of order 2.

Step 3 Calculate the entries of the character table corresponding to χ:

For the element $z \in Z(G) \setminus \{1\} = G' \setminus \{1\}$, we have $\chi_i(z) = \chi_i(1) = 1$ for all $i = \overline{1,4}$. Denote by ρ the regular character. According to the formula in [Isa94, Lemma 2.10 and Lemma 2.11], we have

$$0 = \rho(z) = \sum_{i=1}^{4} \chi_i(1)\chi_i(z) + \chi(1)\chi(z),$$

which leads to $\chi(z) = -2$. Furthermore, $1 = \langle \chi, \chi \rangle = \frac{1}{8} \sum_{g \in G} |\chi(g)|^2$. We have shown that $\chi(1) = 2$ and $\chi(z) = -2$, and therefore $\sum_{g \notin Z(G)} |\chi(g)|^2 = 0$. We conclude that $\chi(g) = 0$ for all $g \in G \setminus Z(G)$.

Step 4 Show that $\det \chi \neq 1_G$ when $G = D_8$:

Let Φ be the representation affording χ. It is routine to verify that $Z(G) = \{1, a^2\}$. It suffices show that $\det \chi(b) = -1$. Since b is non-central, the calculation in Step 3 deduces that $0 = \chi(b) = \mathrm{trace}(\Phi(b))$. On the other side, two eigenvalues of $\Phi(b)$ must be the second root of the unity, i.e. they are either 1 or -1. To sum up, one of them must be 1 and the other is -1, and thus $\det \chi(b) = -1$.

Step 5 Prove that $\det \chi = 1_G$ when $G = Q_8$:

Let Ψ be the representation affording χ. It is routine to verify that $Z(G) = \{1, a^2\}$. Firstly, it is obvious that $\det \chi(1) = 1$. Secondly, since $-2 = \chi(a^2) = \mathrm{trace}\Psi(a^2)$ as mentioned in Step 3 and the fact that every eigenvalue of $\Psi(a^2)$ is the second root of unity, i.e. either 1 or -1, they are both equal to -1, so $\det \chi(a^2) = (-1)^2 = 1$. Finally, note that every element in $G \setminus Z(G)$ is of order 4 and $\chi(g) = 0$ for all $g \in G \setminus Z(G)$ as referred to Step 3. Therefore, two eigenvalues of $\Psi(g)$, where $g \in G \setminus Z(G)$, are respectively $-i$ and i, and so $\det \chi(g) = -i \cdot i = 1$ for all $g \in G \setminus Z(G)$.

Step 6 The completion of the character table of D_8:

Without loss of generality, assume that $\chi_1 = 1_G$. Having all the necessary information above, we complete the character table of D_8 one step of a time. Note that $\{1\}, \{a, a^3\}, \{a^2\}, \{b, ba^2\}$, and $\{ba, ba^3\}$ are all the conjugacy classes of D_8. Firstly, the character χ and the entries of the character table at the center have been computed in Step 3:

D_8	1	a	a^2	b	ba
χ_1	1	1	1	1	1
χ_2	1		1		
χ_3	1		1		
χ_4	1		1		
χ	2	0	-2	0	0

We claim that for each index i, either $\chi_i(g) = 1$ or $\chi_i(g) = -1$ for all elements g. It is sufficient to point it out on the entries of b, ba, and a. Indeed, because each χ_i is a linear character, it is a group homomorphism. Consequently, our claim follows as desired by the equations:

$$\begin{aligned} (\chi_i(a))^2 &= \chi_i(a^2) = 1, \\ (\chi_i(b))^2 &= \chi_i(b^2) = \chi_i(1) = 1, \\ \chi_i(ba) &= \chi_i(b)\chi_i(a). \end{aligned}$$

According to the formula in [Isa94, Lemma 2.10 and Lemma 2.11] once more, we have

$$0 = \rho(a) = \sum_{i=1}^{4} \chi_i(1)\chi_i(a) + \chi(1)\chi(a),$$

which can be reduced to $\chi_2(a) + \chi_3(a) + \chi_4(a) = -1$. Therefore, there are precisely two values of -1 and one value of 1 among the rest three values in the second column. Without loss of generality, we may assume that $\chi_2(a) = 1$ and $\chi_3(a) = \chi_4(a) = -1$.

D_8	1	a	a^2	b	ba
χ_1	1	1	1	1	1
χ_2	1	1	1		
χ_3	1	-1	1		
χ_4	1	-1	1		
χ	2	0	-2	0	0

Next, we have that $0 = \langle \chi_1, \chi_2 \rangle = \frac{1}{8} \sum_{g \in D_8} \chi_1(g)\overline{\chi_2(g)}$, so that

$$-2 = \frac{1}{2}\left(\overline{\chi_2(b)} + \overline{\chi_2(ba)} + \overline{\chi_2(ba^2)} + \overline{\chi_2(ba^3)}\right) = \chi(b) + \chi(ba),$$

which yields that $\chi_2(b) = \chi_2(ba) = -1$.

D_8	1	a	a^2	b	ba
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	1	-1	1		
χ_4	1	-1	1		
χ	2	0	-2	0	0

Using [Isa94, Lemma 2.10 and Lemma 2.11], we have

$$0 = \rho(b) = \sum_{i=1}^{4} \chi_i(1)\chi_i(b) + \chi(1)\chi(b),$$

which leads to $\chi_4(b) = -\chi_3(b)$. Here since the roles of χ_3 and χ_4 are interchangeable, without loss of generality, we may assume that $\chi_3(b) = 1$ and hence $\chi_4(b) = -1$. Finally, we conclude that $\chi_3(ba) = \chi_3(b)\chi_3(a) = 1 \cdot (-1) = -1$, and anologously that $\chi_4(ba) = 1$, which completes the table.

D_8	1	a	a^2	b	ba
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	1	-1	1	1	-1
χ_4	1	-1	1	-1	1
χ	2	0	-2	0	0

Step 7 The completion of the character table of Q_8:

Recall that Q_8 has five conjugacy classes $\{1\}, \{a^2\}, \{a, a^3\}, \{b, ba^2\}$ and $\{ba, ba^3\}$. Assume $\chi_1 = 1_G$. Analogously to the case D_8, we first claim that $\chi_i(g) = 1$ or $\chi_i(g) = -1$ for all elements g and indices i. Indeed, it is proven to be true through the following equations:

$$\begin{aligned}
(\chi_i(a))^2 &= \chi_i(a^2) = 1, \\
(\chi_i(b))^2 &= \chi_i(b^2) = \chi_i(a^2) = 1, \\
\chi_i(ba) &= \chi_i(b)\chi_i(a).
\end{aligned}$$

By the same process as above, we obtain the character table of Q_8:

Q_8	1	a	a^2	b	ba
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	1	-1	1	1	-1
χ_4	1	-1	1	-1	1
χ	2	0	-2	0	0

which resembles the one of D_8.

□

2.4. Let G be a finite group such that $G' \leq Z(G)$ and $|G'| = p$ a prime. Let $\chi \in \operatorname{Irr}(G)$ and $\chi(1) > 1$. Show that χ vanishes on $G \setminus Z(G)$ and $\chi(1)^2 = (G : Z(G))$.

Solution. The conclusion automatically holds if we are able to show that $Z(G) = Z(\chi)$ due to the fact from [Isa94, Corollary 2.30]. Indeed, it follows from [Isa94, Corollary 2.28] that $Z(G) \subseteq Z(\chi)$. Before proving the inverse inclusion, we claim that $G' \cap \ker\chi = 1$. Indeed, either $G' \cap \ker\chi = \{1\}$ or $G' \cap \ker\chi = G'$ since $|G'|$ is a prime number. The latter cannot hold since if otherwise, the irreducible representation affording χ, namely $\mathfrak{X}$, must vanish on G', that is $\mathfrak{X}(g^{-1}h^{-1}gh) = I$ for all $g, h \in G$. Consequently, $\mathfrak{X}(g)\mathfrak{X}(h) = \mathfrak{X}(h)\mathfrak{X}(g)$ for all $g, h \in G$, from which it follows that $\mathfrak{X}(g) = \alpha_g I$ for some $\alpha_g \in \mathbb{C}$ for each $g \in G$ (see [Isa94, Lemma 2.25]). This is impossible since $\mathfrak{X}$ itself is irreducible. For the inverse inclusion, suppose $g \in Z(\chi)$. It follows from [Isa94, Lemma 2.27-(f)] that $g^{-1}h^{-1}gh \in \ker\chi$ for all $h \in G$. Therefore, $g^{-1}h^{-1}gh \in \ker\chi \cap G' = \{1\}$, and hence $g^{-1}h^{-1}gh = 1$ for all $h \in G$, or equivalently $g \in Z(G)$. □

2.5. (a) Let χ be a character of an abelian group A. Show that $\sum_{a\in A}|\chi(a)|^2 \geq |A| \cdot \chi(1)$.
(b) Let G be a finite group with an abelian subgroup A. Show that $\chi(1) \leq [G : A]$ for any $\chi \in \operatorname{Irr}(G)$.

Solution. (a) Denote by $\operatorname{Irr}(A)$ the set of all irreducible characters of A and suppose $\operatorname{Irr}(A) = \{\chi_1, \ldots, \chi_k\}$. Since χ is a character of A, there are nonnegative integers $n_1, \ldots, n_k$ such that $\chi = \sum_{i=1}^k n_i\chi_i$. Note that $\chi_i(1) = 1$ for all indices i because of the fact that A is abelian. We now consider two ways of computing $\langle\chi, \chi\rangle$. Firstly, it comes from the definition that

$$\langle\chi, \chi\rangle = \frac{1}{|A|}\sum_{a\in A}|\chi(a)|^2.$$

Secondly, we have

$$\begin{aligned}
\langle\chi, \chi\rangle &= \left\langle \sum_{i=1}^k n_i\chi_i, \sum_{j=1}^k n_j\chi_j \right\rangle \\
&= \sum_{i=1}^k\sum_{j=1}^k n_in_j\langle\chi_i, \chi_j\rangle \\
&= \sum_{i=1}^k n_i^2 \\
&\geq \sum_{i=1}^k n_i = \sum_{i=1}^k n_i\chi_i(1) = \chi(1).
\end{aligned}$$

We conclude that

$$\frac{1}{|A|}\sum_{a\in A}|\chi(a)|^2 \geq \chi(1), \text{ or equivalently, } \sum_{a\in A}|\chi(a)|^2 \geq |A|\cdot\chi(1).$$

(b) Let χ be an irreducible character of G. Because χ_A is a character of an abelian group A, we deduce from (a) that $|A|\cdot\chi_A(1) \leq \sum_{a\in A}|\chi_A(a)|^2$, which leads to

$$|A|\cdot\chi(1) \leq \sum_{a\in A}|\chi(a)|^2 \leq \sum_{g\in G}|\chi(g)|^2 = |G|\frac{1}{|G|}\sum_{g\in G}|\chi(g)|^2 = |G|\langle\chi,\chi\rangle = |G|,$$

where the last equality holds because of irreducibility of χ. Hence, we conclude that $\chi(1) \leq \frac{|G|}{|A|} = [G:A]$.

□

3.1. Show that no simple group can have an irreducible character of degree 2.

Solution. Prior to solving the exercise, we state the following result.

Lemma 2. *Let G be a simple non-abelian group. Then, the principal character 1_G is the unique linear character of G. Moreover, if χ is any non-principal irreducible character of G, then* $\ker\chi = 1$.

Proof of Lemma 2. Denote by G' the commutator subgroup of G. Then, $G' \trianglelefteq G$ and $G' \neq 1$ (because G is not abelian), which means $G' = G$ (because G is simple). Besides, it is known (see [Isa94, Corollary 2.23]) that the number of linear characters of G equals $[G:G'] = 1$, from which we deduce that there is only one linear character of G, i.e. the principal 1_G is the unique character of degree 1 of G.

In addition, let $\chi \neq 1_G$ be an irreducible character of G and assume by contradiction that $\ker\chi \neq 1$. We have $1 = \langle\chi,\chi\rangle = \frac{1}{|G|}\sum_{g\in G}|\chi(g)|^2$, and so $|G| = \sum_{g\in G}|\chi(g)|^2$. Since $1 \neq \ker\chi \triangleleft G$, $\ker\chi$ must be equal to G, implying that $|G| = \sum_{g\in G}|\chi(g)|^2 = |G||\chi(1)|^2$ and hence $\chi(1) = 1$. We have shown that $\chi \neq 1_G$ is a character of degree 1 of G, which contradicts to the assertion above. Hence, $\ker\chi = 1$ and the proof of the lemma is complete. □

We may now solve the problem. Let G be a simple group and assume by contradiction that there exists an irreducible character χ of degree 2 which is afforded by a representation Φ. It follows that G is non-abelian because all irreducible characters of an abelian group are linear. Since $2 = \chi(1)$ is a divisor of $|G|$ (see [Isa94, Theorem 3.11]), it turns out that G has even order. According to Cauchy's Lemma, G has an element j of order 2. Then, it follows from [Isa94, Lemma 2.15] that $\Phi(j)$ is similar to a diagonal matrix $\begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix}$ and $\chi(j) = a_1 + a_2$ where a_1 and a_2 are equal to either -1 or 1. Recall from [Isa94, Exercise 2.3] that the map $\det\chi : G \to \mathbb{C}$ defined as $\det\chi(g) = \det(\Phi(g))$, for all $g \in G$, is a linear character of G. According to the Lemma 2, $\det\chi$ is in fact the principal character, i.e. $\det\chi \equiv 1_G$. Consequently, $1 = \det\chi(j) = \det(\Phi(j)) = a_1a_2$ or equivalently, either $a_1 = a_2 = 1$ or $a_1 = a_2 = -1$. If $a_1 = a_2 = 1$, then $\chi(j) = 2 = \chi(1)$ and $j \in \ker\chi$, contradicting to the above lemma. Therefore, $a_1 = a_2 = -1$ and $\Phi(j)$ is similar to the matrix $-I_2$, so $\Phi(j) = -I_2$. Additionally, observe that Φ is injective. Indeed, we have $\ker\Phi \triangleleft G$, so either $\ker\Phi = 1$ or $\ker\Phi = G$, the latter case of which does not happen because $\Phi(j) = -I_2 \neq I_2$. Now that $\Phi(jg) = \Phi(j)\Phi(g) = \Phi(g)\Phi(j) = \Phi(gj)$ for all $g \in G$ and Φ is injective, we deduce that $jg = gj$ for all $g \in G$, and so $j \in Z(G)$. This means that $1 \neq Z(G) \trianglelefteq G$, so that $Z(G) = G$ or equivalently, G is abelian. A contradiction! In summary, the simple group G does not possess any irreducible character of degree 2 and our proof is complete.

□

3.2. Let G be a finite group of odd order.

(a) Let $\chi \in \mathrm{Irr}(G)$ and suppose χ is not the principal character. Show that χ and its complex conjugate $\overline{\chi}$ are different.
(b) Suppose G has exactly r conjugacy classes. Show that $|G| \equiv r \mod 16$.

Solution. (a) Because of the oddness of $|G|$, there are no elements of G having order 2. This means that if $a \in G\backslash\{1\}$, then $a^{-1} \neq a$, so we can write $G = \{1\} \sqcup \{a_1, a_1^{-1}\} \sqcup \cdots \sqcup \{a_m, a_m^{-1}\}$ as disjoint union of subsets, where $m = \frac{|G|-1}{2}$. Assume by contradiction that $\chi \neq 1_G$ is an irreducible chracter such that $\chi = \overline{\chi}$. Then we obtain $\chi(a_i^{-1}) = \overline{\chi}(a_i) = \chi(a_i)$ for all $1 \leq i \leq m$. Since $\chi \neq 1_G$, we have

$$0 = \langle \chi, 1_G \rangle = \frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{1_G}(g) = \frac{1}{|G|} \sum_{g \in G} \chi(g) = \frac{1}{|G|}(\chi(1) + 2 \cdot \sum_{i=1}^{m} \chi(a_i)),$$

which is equivalent to $\frac{\chi(1)}{2} = -\sum_{i=1}^m \chi(a_i)$. By [Isa94, Corollary 3.5 and Corollary 3.6], $\frac{\chi(1)}{2}$ is an algebraic integer. In addition, $\frac{\chi(1)}{2}$ is a rational number, then, according to [Isa94, Lemma 3.2], $\frac{\chi(1)}{2} \in \mathbb{Z}$, so $\chi(1)$ is an even number. Using [Isa94, Theorem 3.11], we have $2 \mid \chi(1) \mid |G|$. A contradiction!

(b) According to [Isa94, Corollary 2.7], there are exactly r irreducible characters of G, namely $\chi_1 = 1_G, \chi_2, \dots, \chi_r$. By [Isa94, Theorem 3.11], we imply that $\chi_i(1)$ is an odd number for all $1 \leq i \leq r$. According to part (a), $\chi_i \neq \overline{\chi_i}$ where $1 \leq i \leq r$, so r is an odd number. Without loss of generality, by renumbering the indices if necessary, we can assume that $\chi_i \neq \overline{\chi_j}$ for all $2 \leq i, j \leq \frac{r+1}{2}$. Recall that the complex conjugate of an irreducible character is an irreducible character. Then the characters $\left\{\overline{\chi_{\frac{r+1}{2}+1}}, \dots, \overline{\chi_r}\right\}$ are a permutation of $\left\{\chi_1, \dots, \chi_{\frac{r+1}{2}}\right\}$.

$$\begin{aligned}
|G| - r &= \sum_{i=1}^{r} \chi_i(1)^2 - r \\
&= \sum_{i=2}^{r} (\chi_i(1)^2 - 1) \\
&= \sum_{i=2}^{\frac{r+1}{2}} (\chi_i(1)^2 - 1) + \sum_{k=\frac{r+1}{2}+1}^{r} (\chi_k(1)^2 - 1) \\
&= \sum_{i=2}^{\frac{r+1}{2}} (\chi_i(1)^2 - 1) + \sum_{k=2}^{\frac{r+1}{2}} (\overline{\chi_k(1)}^2 - 1) \\
&= 2\sum_{i=2}^{\frac{r+1}{2}} (\chi_i(1)^2 - 1)
\end{aligned}$$

Recall that $n^2 \equiv 1 \mod 8$ for all odd integer n, so $8 \mid \chi_i(1)^2 - 1$ for all $2 \leq i \leq \frac{r+1}{2}$. Therefore, $16 \mid 2\sum_{i=2}^{\frac{r+1}{2}} (\chi_i(1)^2 - 1) = |G| - r$ as desired.

□

3.3. Let G be a non-abelian group of order p^3, where p is a prime integer. Show that G has exactly $p^2 + p - 1$ irreducible characters: p^2 of degree 1 and $p - 1$ of degree p.

Solution. Imitating the initial arguments in Problem 2.3, we obtain $[G, G] = Z(G)$ and $|Z(G)| = p$. As stated in [Isa94, Theorem 3.11] and as the fundamental formula $|G| = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2$, $\chi(1)$ is equal to either 1 or p for all $\chi \in \mathrm{Irr}(G)$. By [Isa94, Lemma 2.22], G has exactly $[G : [G, G]] = p^2$ linear characters. Thus, there are exactly $\frac{p^3-p^2}{p^2} = p-1$ irreducible characters of order p. They are all irreducible characters of G. The proof is complete. $\square$

3.4. Let G be a simple group having an irreducible character χ of prime degree p. Show that p, but not p^2, divides $|G|$.

Solution. The following result tells us one way to determine whether a subgroup is abelian by looking at its constituent of the restriction character. It is already referred to [Isa94, Excersise 2.8], but we include a proof here for completeness.

Lemma 3. *Let χ be a faithful character of G. Then, $H \leq G$ is abelian iff every irreducible constituent of χ_H is linear.*

Proof of Lemma 3. It is obvious that if H is abelian, then every its irreducible character is linear. For the converse part, assume $\chi_H = n_1\tau_1 + \cdots + n_k\tau_k$ where $n_i \geq 1$ and $\tau_i \in \mathrm{Irr}(H)$ of degree 1. Note that since χ is faithful, so is χ_H, which means that $\ker \chi_H = 1$. By [Isa94, Lemma 2.21], $\bigcap_{i=1}^k \ker \tau_i = \ker \chi_H = 1$ as above. On the other hand, according to [Isa94, Corolarry 2.23], $[H, H] \subseteq \bigcap_{i=1}^k \ker \tau_i = 1$ because of the linearities of $\ker \tau_i$'s. Thus, $[H, H] = 1$. In other words, H is abelian, and the proof is complete. $\square$

It is known that $\chi(1) \mid |G|$, so $p = \chi(1)$ is a divisor of $|G|$. The rest of the proof is to show that $p^2 \nmid |G|$.

First, observe that χ is a faithful character. Indeed, if it is not faithful, then $1 \neq \ker \chi \trianglelefteq G$, which leads to $\ker \chi = G$ because of simplicity of G. But then, $|G| = \sum_{g\in G} |\chi(g)|^2 = |G||\chi(1)|^2$ and $\chi(1) = 1$, which contradicts to the assumption that $\chi(1) = p$ is a prime number. Hence, χ is a faithful irreducible character of degree p. We also note that G is non-abelian, so $Z(G) = 1$ as the simplicity of G.

Let P be a Sylow p-subgroup of G. We will show that P is abelian. Assume by contradiction that P is non-abelian. Applying Lemma 3, the restriction $\chi_P : P \to \mathbb{C}$ is a character of P having a non-linear irreducible constituent. To make it clear, suppose that $\mathrm{Irr}(P) = \{\tau_1, \ldots, \tau_r\}$, then $\chi_P = \sum_{i=1}^r n_i\tau_i$ for some nonnegative integers $n_1, \ldots, n_r$ and furthermore, there exists some index j such that $0 < n_j$ and $1 < \tau_j(1)$. Since $\tau_j(1) > 1$ is a divisor of $|P|$, which is a power of p, $\tau_j(1)$ must be divisible by p. Therefore, $p = \chi_P(1) = \sum_{i=1}^r n_i\tau_i(1) \geq n_j\tau_j(1) \geq n_jp \geq p$. Consequently, $n_j = 1$ and $n_i = 0$ for all $i \neq j$, so $\chi_P = \tau_j$ is an irreducible character of P. Let x be an arbitrary element in $Z(P)$ and $\mathfrak{X}$ be an irreducible representation of P affording χ_P. Then $\mathfrak{X}(x)$ is a $p \times p$ matrix over $\mathbb{C}$ which commutes with $\mathfrak{X}(y)$ for all $y \in P$. By [Isa94, Lemma 2.25], this means that $\mathfrak{X}(x) = \lambda I_p$ for some $\lambda \in \mathbb{C}$ such that λ is an $|x|$-th root of unity, which implies that $x \in Z(\chi)$. We have just shown that $Z(P) \leq Z(\chi) = Z(G) = 1$ by [Isa94, Lemma 2.27(f)], provided that χ is a faithful irreducible character. We deduce that $Z(P) = 1$, which is a contradiction because it is well-known that the center of a p-group is always non-trivial. Therefore, the Sylow p-subgroup P must be abelian. Then, by [Isa94, Theorem 3.13], $p \mid |G|$ but $p^2 \nmid |G|$ and our proof is complete. $\square$

3.5. Show that any finite non-abelian simple group has order at least 60.

Solution. We begin with the remark that every non-abelian simple group is not solvable. According to Burnside's p^aq^b-theorem, every group whose order of the form p^aq^b is solvable. As a consequence, every group of order less than 60, excluding those of orders 30 and 42, is solvable, and hence either abelian or not simple. Now, consider the excluding cases:

- Assume G be a finite group of order $30 = 2 \times 3 \times 5$. Let n_p denote the number of p-Sylow subgroups of G. We claim that G is not simple. If otherwise, every n_p must be different from 1 since if otherwise, the only p-Sylow subgroup of G is normal in G, which is a contradiction. By using the argument in Sylow theorems, that is, $n_p \equiv 1 \mod p$ and $n_p \mid |G|$, we deduce

that there are 10 subgroups of order 3 and 6 subgroups of order 5. Furthermore, all of these subgroups must be cyclic, so every non-trivial element of such groups generates the whole one. However, each of these elements is contained in only one such a subgroup. Therefore, there are at least $6 \times (5-1) + 10 \times (3-1) = 44$ elements in G. A contradiction!
- As above, suppose that G be a finite simple group of order $42 = 2 \times 3 \times 7$. By Sylow theorems, it follows that $n_7 = 1$ since $n_7 \equiv 1 \mod 7$ and $n_7 \mid 6$. A contradiction to the simplicity.

In conclusion, every finite group having order less than 60 must be either abelian or non-simple. □

3.6. Let g be an element of a finite group G and let k be any integer coprime to $|g|$. Show that g is a commutator in G if and only if g^k is a commutator in G.

Solution.

Lemma 4. *Let $\mathcal{K}_1, \dots, \mathcal{K}_k$ be the conjugacy classes of a group G and let $K_1, \dots, K_k$ be the corresponding class sums. Choose representatives $g_i \in \mathcal{K}_i$ and let a_{ijv} be the nonnegative integers (see [Isa94, Theorem 2.4]) defined by*

$$K_i K_j = \sum_v a_{ijv} K_v.$$

Then, we have

$$a_{ijv} = \frac{|\mathcal{K}_i||\mathcal{K}_j|}{|G|} \sum_{\chi \in Irr(G)} \frac{\chi(g_i)\chi(g_j)\overline{\chi(g_v)}}{\chi(1)}.$$

Proof of Lemma 4. Since ω_χ is an algebra homomorphism from $Z(\mathbb{C}G)$ to $\mathbb{C}$, we have

$$\omega_\chi(K_i)\omega_\chi(K_j) = \sum_v a_{ijv}\omega_\chi(K_v), \text{ or } \frac{\chi(g_i)|\mathcal{K}_i|}{\chi(1)} . \frac{\chi(g_j)|\mathcal{K}_j|}{\chi(1)} = \sum_v a_{ijv} \frac{\chi(g_v)|\mathcal{K}_v|}{\chi(1)},$$

which can be reduced to

$$\frac{|\mathcal{K}_i||\mathcal{K}_j|\chi(g_i)\chi(g_j)}{\chi(1)} = \sum_v a_{ijv}|\mathcal{K}_v|\chi(g_v).$$

Fix some v. By multiplying with $\overline{\chi(g_v)}$ on both sides of the above equation and summing it up with respect to irreducible characters, we conclude that

$$\begin{aligned} |\mathcal{K}_i||\mathcal{K}_j| \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g_i)\chi(g_j)\overline{\chi(g_v)}}{\chi(1)} &= a_{ijv}|\mathcal{K}_v| \sum_{\chi \in \mathrm{Irr}(G)} |\chi(g_v)|^2 + \sum_{w \neq v} a_{ijw}|\mathcal{K}_w| \sum_{\chi \in \mathrm{Irr}(G)} \chi(g_w)\overline{\chi(g_v)} \\ &= a_{ijv}|\mathcal{K}_v||C_G(g_v)| \\ &= |G|a_{ijv}, \end{aligned}$$

where the third equation is derived from the second orthogonality relation in [Isa94, Theorem 2.18]. □

Lemma 5. *We write $[x, y]$ for the* commutator $x^{-1}y^{-1}xy$ *of x and y in a group G.*

(a) *Let $g \in G$ and fix $x \in G$. Then, g is conjugate to $[x, y]$ for some $y \in G$ iff*

$$\sum_{\chi \in Irr(G)} \frac{|\chi(x)|^2\chi(g)}{\chi(1)} \neq 0.$$

(b) *$g = [x, y]$ for some $x, y \in G$ iff*

$$\sum_{\chi \in Irr(G)} \frac{\chi(g)}{\chi(1)} \neq 0.$$

Proof of Lemma 5. We use the notions as in Lemma 4.

(a) Notice that from Lemma 4, the required sum must be non-negative. Suppose that $g = [x,y]^h = [x^h, y^h]$ for some $h \in G$. Without loss of generality, we assume that $g \in \mathcal{K}_i$ and $\{x, x^h\} \subseteq \mathcal{K}_j$. Then, we have that $0 < a_{jij}$ since $x^h g = (y^h)^{-1} x^h y^h = (x^h)^{y^h} \in \mathcal{K}_j$. Applying this remark with Lemma 4, we deduce that

$$0 < \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(x^h)\chi(g)\overline{\chi(x^h)}}{\chi(1)} = \sum_{\chi \in \mathrm{Irr}(G)} \frac{\left|\chi\left(x^h\right)\right|^2 \chi(g)}{\chi(1)} = \sum_{\chi \in \mathrm{Irr}(G)} \frac{|\chi(x)|^2 \chi(g)}{\chi(1)}.$$

Conversely, suppose that

$$0 < \sum_{\chi \in \mathrm{Irr}(G)} \frac{|\chi(x)|^2 \chi(g)}{\chi(1)} = \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(x)\chi(g)\overline{\chi(x)}}{\chi(1)},$$

and $g \in \mathcal{K}_i$ and $x \in \mathcal{K}_j$. It follows that $0 < a_{jij}$, which leads to $x^u g^v = x^w$ for some $u, v, w \in G$, or equivalently

$$g^{vu^{-1}} = u(x^u)^{-1} x^w u^{-1} = x^{-1} u w^{-1} x w u^{-1} = x^{-1}(wu^{-1})^{-1} x w u^{-1} = [x, wu^{-1}].$$

(b) Assume that $g = [x,y]$ for some x, y. By Lemma 5(a), for each $z \in G$, either

$$0 = \sum_{\chi \in \mathrm{Irr}(G)} \frac{|\chi(z)|^2 \chi(g)}{\chi(1)},$$

or

$$0 < \sum_{\chi \in \mathrm{Irr}(G)} \frac{|\chi(z)|^2 \chi(g)}{\chi(1)},$$

and there must be at least one z, e.g. when $z = x$, where the latter relation holds. Summing it up with respect to z over G, we obtain that

$$0 < \sum_{z \in G} \sum_{\chi \in \mathrm{Irr}(G)} \frac{|\chi(z)|^2 \chi(g)}{\chi(1)} = \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g)}{\chi(1)} \sum_{z \in G} |\chi(z)|^2 = |G| \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g)}{\chi(1)} \tag{3}$$

and hence the conclusion.

Conversely, the sum as in (3) is positive. It implies that there exists some $z \in G$ such that

$$0 < \sum_{\chi \in \mathrm{Irr}(G)} \frac{|\chi(z)|^2 \chi(g)}{\chi(1)},$$

from which follows that $g = [z,y]^w = [z^w, y^w]$.

$\square$

Back to our main problem, it is sufficient to only prove the "only if" part. The assumption can be rephrased into

$$\sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g)}{\chi(1)} \neq 0,$$

from Lemma 5(b). Let $|g| = n$, and let E be the splitting field of $x^n - 1$ over $\mathbb{Q}$. Denote by $\mathcal{G}$ the Galois group of E over $\mathbb{Q}$, and $\varepsilon \in E$ a n-th root of unity. As k is coprime to $|g|$, there is an element σ of $\mathcal{G}$ determined by

$$\begin{aligned} \sigma : E &\to E, \\ \varepsilon &\mapsto \varepsilon^k. \end{aligned}$$

Then, for each irreducible character χ, we have $\chi(g) = \varepsilon^{i_1} + \cdots + \varepsilon^{i_m}$ for some $m \in \mathbb{N}$. It implies that

$$\chi(g)^\sigma = (\varepsilon^{i_1})^\sigma + \cdots + (\varepsilon^{i_m})^\sigma = \varepsilon^{k i_1} + \cdots + \varepsilon^{k i_m} = \chi(g^k).$$

Consequently,

$$0 \neq \left(\sum_{\chi\in\mathrm{Irr}(G)} \frac{\chi(g)}{\chi(1)}\right)^{\sigma} = \sum_{\chi\in\mathrm{Irr}(G)} \left(\frac{\chi(g)}{\chi(1)}\right)^{\sigma} = \sum_{\chi\in\mathrm{Irr}(G)} \frac{\chi(g^k)}{\chi(1)},$$

or that g^k is a commutator in G. □

4.1. Let G be a finite group having a subgroup H of prime index p. Suppose p is the smallest prime divisor of $|G|$. Show that $H \lhd G$.

Solution. Firstly, we will prove the following claim: If $a \notin H$, then the collection $\{H, aH, \dots, a^{p-1}H\}$ forms the left cosets of H in G. Indeed, any prime divisor of $|a|$ must not be less than p. As a result, given $i \in \{1, \dots, p-1\}$, then i is coprime with $|a|$ and consequently, there exists integers u and v satisfying $ui + v|a| = 1$. Hence, $a^{ui} = a^{ui+v|a|} = a \notin H$, implying that $a^i \notin H$. It follows that $a^iH \neq a^jH$ for all $i, j \in \{0, \dots, p-1\}$ such that $i \neq j$. Since $p = [G : H]$, we deduce the above assertion.

Now choose $g \in G$ and $h \in H$ arbitrarily, the aim is to show that $g^{-1}hg \in H$. Assume by contradiction that $g^{-1}hg \notin H$, then $G/H = \{(g^{-1}h^ig)H : 0 \leq i \leq p-1\}$ because of the aforementioned assertion. Then, $g^{-1}H = (g^{-1}h^jg)H$ for some index j, so $h^jg \in H$, or equivalently $g \in H$. As a consequence, we must have $g^{-1}hg \in H$, a contradiction! Therefore, $g^{-1}hg \in H$ for all $g \in G$ and $h \in H$ as desired. □

4.2. Let χ, ψ be characters of a finite group G. Prove that $\det(\chi\psi) = (\det\chi)^{\psi(1)}(\det\psi)^{\chi(1)}$.

Proof. We need to prove that $\det(\chi\psi)(g) = (\det\chi(g))^{\psi(1)}(\det\psi(g))^{\chi(1)}$ for all $g \in G$. Let V, W be $\mathbb{C}G$-modules affording to χ, ψ, respectively, so $V \otimes W$ is the $\mathbb{C}G$-module affording to $\chi\psi$. We regard $V, W, V \otimes W$ as $\mathbb{C}\langle g\rangle$-modules by the restriction of G to $\langle g\rangle$. We decompose $V = V_1 \oplus \cdots \oplus V_n$ and $W = W_1 \oplus \cdots \oplus W_m$ into irreducible $\mathbb{C}\langle g\rangle$-modules. As $\langle g\rangle$ is abelian, all the V_i's and W_j's are one-dimensional spaces, that is, $V_i = \mathbb{C}v_i$ and $W_j = \mathbb{C}w_j$ for all $1 \leq i \leq n, 1 \leq j \leq m$, so $\chi(1) = \dim_{\mathbb{C}} V = n$ and $\psi(1) = \dim_{\mathbb{C}} W = m$. In the other words, $\{v_i\}_{i=1}^n$ and $\{w_j\}_{j=1}^m$ are $\mathbb{C}$-bases of V and W respectively, so $\{v_i \otimes w_j : 1 \leq i \leq n, 1 \leq j \leq m\}$ is a basis of $V \otimes W$. If we write $v_ig = a_iv_i$ and $w_jg = b_jw_j$, we have $(v_i \otimes w_j)g = a_ib_j(v_i \otimes w_j)$. Thus, the matrix formed by the action of g on $V \otimes W$ over the basis is a diagonal matrix of degree $nm \times nm$ whose $((i,j),(i,j))$-th entry is equal to a_ib_j. Note that $\det(\chi\psi)(g)$ is the determinant of this matrix, and furthermore $\det\chi(g) = \prod_{i=1}^n a_i$ and $\det\psi(g) = \prod_{j=1}^m b_j$. Hence

$$\det(\chi\psi)(g) = \prod_{(i,j)\in\{1,\dots,n\}\times\{1,\dots,m\}} a_ib_j = \left(\prod_{i=1}^n a_i\right)^m \left(\prod_{j=1}^m b_j\right)^n = (\det\chi(g))^{\psi(1)}(\det\psi(g))^{\chi(1)},$$

as desired. The proof is complete. □

4.3. Let $G = H \times K$ be the direct product of two finite groups H, K. Let $\alpha \in \mathrm{Irr}(H)$ and $\beta \in \mathrm{Irr}(K)$ be faithful. Show that $\alpha \times \beta$ is faithful if and only if $(|Z(H)|, |Z(K)|) = 1$.

Solution. As stated in [Isa94, Lemma 2.27-(d)-(f)], provided that α and β are faithful irreducible characters of H and K, respectively, we obtain that

$$Z(H) = Z(\alpha) = \{h \in H : |\alpha(h)| = \alpha(1)\}, \text{ and } Z(K) = Z(\beta) = \{k \in K : |\beta(k)| = \beta(1)\}$$

are cyclic groups. Denote by h and k the generators of $Z(H)$ and $Z(K)$, respectively. Let ρ_H, ρ_K denote the representation of H and K affording α and β, respectively.

($\Rightarrow$) Suppose the product character $\alpha \times \beta$ is faithful and set $d = (|h|, |k|) = (|Z(H)|, |Z(K)|)$. Then, the fact that $h \in Z(H)$ yields $\rho_H(h) = \varepsilon I_{\alpha(1)}$, where $\varepsilon \in \mathbb{C}$ such that $\varepsilon^{|h|} = 1$ (referred to [Isa94, Lemma 2.25]). Furthermore, it turns out that ε is a primitive $|h|$-th root of unity, i.e. $|h|$ is the smallest positive integer such that $\varepsilon^{|h|} = 1$. Indeed, if n is the order of ε, then it is obvious that

$n \mid |h|$. On the other hand, we derive that $n = |h|$ since $\rho_H(h^n) = I_{\alpha(1)} = \rho_H(1)$ and ρ is faithful. Thus, ε is a primitive $|h|$-th root of unity, which implies $\varepsilon^{\frac{|h|}{d}}$ is a primitive d-th root of unity. By a similar argument, we have $\rho_K(k) = \delta I_{\beta(1)}$ such that $\delta^{\frac{|k|}{d}}$ is a primitive d-th root of unity. Therefore, there exists $m \in \mathbb{Z}$ such that $\varepsilon^{\frac{|h|}{d}} = \delta^{-\frac{|k|}{d}m}$, which means $\varepsilon^{\frac{|h|}{d}}\delta^{\frac{|k|}{d}m} = 1$. As a result, we have

$$\begin{aligned}(\alpha\times\beta)\left(h^{\frac{|h|}{d}}\cdot k^{m\frac{|k|}{d}}\right) &= \alpha\left(h^{\frac{|h|}{d}}\right)\beta\left(k^{\frac{|k|m}{d}}\right)\\ &= \varepsilon^{\frac{|h|}{d}}\delta^{m\frac{|k|}{d}}\alpha(1)\beta(1)\\ &= (\alpha\times\beta)(1\cdot 1),\end{aligned}$$

indicating that $x^{\frac{|h|}{d}} = k^{m\frac{|k|}{d}} = 1$ due to faithfulness of $\alpha\times\beta$. This means that $d = 1$ as our wish.

($\Leftarrow$) Now suppose $(|Z(H)|, |Z(K)|) = 1$. Let $h \in H$, $k \in K$ satisfy $h \cdot k \in \ker(\alpha\times\beta)$. Then, $\alpha(h)\beta(k) = (\alpha\times\beta)(h\cdot k) = (\alpha\times\beta)(1\cdot 1) = \alpha(1)\beta(1)$. Hence, $|\alpha(h)\beta(k)| = \alpha(1)\beta(1)$. Combining this with the fact that $|\alpha(h)| \le \alpha(1)$ and $|\beta(k)| \le \beta(1)$, we obtain $|\alpha(h)| = \alpha(1)$ and $|\beta(k)| = \beta(1)$, or equivalently that $h \in Z(\alpha) = Z(H)$ and $k \in Z(\beta) = Z(K)$ according to [Isa94, Lemma 2.27-(f)].

Again, by [Isa94, Lemma 2.25], $\rho_H(h) = \varepsilon I_{\alpha(1)}$ and $\rho_K(k) = \delta I_{\beta(1)}$ for some complex numbers ε, δ. Using analogous argument as the "only if" part, we obtain that ε and δ have the order $|h|$ and $|k|$, respectively. We have $\alpha(h) = \varepsilon\alpha(1)$, $\beta(k) = \delta\beta(1)$, so

$$\alpha(1)\beta(1) = (\alpha\times\beta)(1\cdot 1) = (\alpha\times\beta)(h\cdot k) = \alpha(h)\beta(k) = \varepsilon\delta\alpha(1)\beta(1),$$

which means that $\varepsilon\delta = 1$ as $\alpha(1)$ and $\beta(1)$ are nonzero. It is routine to verify that ε and δ have the common order, i.e. $|h| = |k|$. In addition, the condition $(|Z(H)|, |Z(K)|) = 1$ asserts that $(|h|, |k|) = 1$ since $|h| \mid |Z(H)|$ and $|k| \mid |Z(K)|$. Combine the above statement, $|h| = |k| = (|h|, |k|) = 1$, which means $h = k = 1$. The proof is complete. □

4.4. Let G be a finite group generated by two involutions x, y. Show that if $z = xy$ has order $n > 2$ then

$$G = \langle x, z : x^2 = z^n = 1, xzx^{-1} = z^{-1}\rangle$$

is the dihedral group of order $2n$. Show that

(a) If n is odd, then any two involutions in G are conjugate.
(b) If n is even, then $Z(G)$ has order 2; namely, it is generated by $z^{\frac{n}{2}}$.
(c) Determine the character table of G.

Solution. It follows that $G = \langle x, z\rangle$ by the remark that $z = xy \in \langle x, y\rangle$ and $y = x^{-1}z \in \langle x, z\rangle$. Since $x^2 = 1 = y^2$, we have $xzx^{-1} = x(xy)x^{-1} = yx^{-1} = y^{-1}x^{-1} = (xy)^{-1} = z^{-1}$. Therefore,

$$G = \langle x, z : x^2 = z^n = 1, xzx^{-1} = z^{-1}\rangle = D_{2n}.$$

Remark that every element of G has the form of x^iz^j for some indices $0 \le i \le 1$ and $0 \le j \le n-1$. Because of that, for the rest of the proof, when we write x^iy^j, we always assume that $0 \le i \le 1$ and $0 \le j \le n-1$. Moreover, it is useful to keep in mind the following formula: for any integer j, we have $xz^j = z^{-j}x$.

(a) Consider the case when n is odd. In this case, there are precisely n involutions of G which are all elements having the form xz^j with. Indeed, observe that $xz^j \ne 1$ and $(xz^j)^2 = xz^jxz^j = z^{-j}z^j = 1$. Besides, if there exists z^j as an involution of G, then $z^{2j} = 1 = z^n$, indicating that $n \mid 2j$. Then, $n \mid j$ because n is odd, which implies $j = 0$, so $z^0 = 1$ is an involution, a contradiction! Now consider the centralizer $C(x)$ of x. If $x^iz^j \in C(x)$, then $x = (x^iz^j)^{-1}x(x^iz^j) = xz^{2j}$, so $z^{2j} = 1$, which only happens when $j = 0$ as shown above. Therefore, $C(x) = \{1, x\}$. It implies that $\left|x^G\right| = \frac{|G|}{|C(x)|} = \frac{2n}{2} = n$. Also, notice that all n elements of x^G are involutions because x is itself an involution. We deduce that all involutions of G belong to x^G, and thus any two involutions are conjugate, since both are conjugate to x.

(b) Consider the case when n is even. By arguing similarly to part (a), if $x^i z^j \in C(x)$, then $n \mid 2j$, which means either $j = 0$ or $j = \frac{n}{2}$. Thus, $C(x) \subseteq \{1, x, z^{\frac{n}{2}}, xz^{\frac{n}{2}}\}$, implying that $Z(G) \subset C(x) \subset \{1, x, z^{\frac{n}{2}}, xz^{\frac{n}{2}}\}$. However, it is routine to check that $xz \neq zx$ and $(xz^{\frac{n}{2}})z^{\frac{n}{2}+1} \neq z^{\frac{n}{2}+1}(xz^{\frac{n}{2}})$ where the condition $n > 2$ is applied, so x and $xz^{\frac{n}{2}}$ are non-central. Moreover, since $z^{\frac{n}{2}}x = xz^{-\frac{n}{2}} = xz^{\frac{n}{2}}$, $z^{\frac{n}{2}}$ commutes with x, and thus it commutes with all elements in $\langle x, z\rangle = G$. We deduce that $Z(G) = \{1, z^{\frac{n}{2}}\}$ and $|Z(G)| = 2$.

(c) We mainly focus on constructing the character table of D_{2n} when n is odd. The other case is dealt with similarly. We recall the following result which determines all conjugacy classes of D_{2n}:

Lemma 6. *If n is odd, then there are precisely $\frac{n+3}{2}$ conjugacy classes of D_{2n} given as follows:*

$$\{1\}, \{z, z^{n-1}\}, \{z^2, z^{n-2}\}, \dots, \{z^{\frac{n-1}{2}}, z^{\frac{n+1}{2}}\}, \{x, xz, xz^2, \dots, xz^{n-1}\}.$$

Proof of Lemma 6. It is already shown at the beginning of the solution that x^G consisting of all elements of the form xy^j is a conjugacy class containing all involutions of D_{2n}. In addition, for each $1 \leq k \leq \frac{n-1}{2}$, observe that

$$\begin{aligned}(z^k)^G &= \{g^{-1}z^k g : g \in G\} \\ &= \{z^{-j}z^k z^j : 1 \leq j \leq n-1\} \cup \{(xz^j)^{-1}z^k(xz^j) : 1 \leq j \leq n-1\} \\ &= \{z^k, z^{-k}\},\end{aligned}$$

which completes the proof of Lemma 6. □

It follows immediately from the lemma that there are precisely $\frac{n+3}{2}$ irreducible characters of G. Let χ_1 be the principal character 1_G. Since G has n involutions, [Isa94, Theorem 4.11] asserts the existence of an irreducible character $\chi_2 \neq 1_G$ such that $\chi_2(1) \leq \frac{|G|-1}{n} = \frac{2n-1}{n} < 2$ (moreover, it is real-valued). In other words, there exists another irreducible linear character χ_2 of G apart from 1_G. Since $(\chi_2(z))^n = \chi_2(z^n) = \chi_2(1) = 1$ and $\chi_2(z)^{-1} = \chi_2(z^{-1}) = \chi_2(xzx) = \chi_2(x)^2\chi_2(z) = \chi_2(z)$, it turns out that $\chi_2(z) = \chi_2(z)^n(\chi_2(z)^{-2})^{\frac{n-1}{2}} = 1$. Besides, $\chi_2(x)$ must be -1 (if $\chi_2(x) = 1$ then χ_2 would be identical to 1_G). In particular, $\chi_2(x^i z^j) = (-1)^i$ for all i, j. The argument above also leads to the uniqueness of the non-principal linear character, it means that there are only two irreducible characters of degree 1 of G. Put $\mathrm{Irr}(G) = \{\chi_1, \chi_2, \chi_3, \dots, \chi_{\frac{n+3}{2}}\}$, then

$$2n = |G| = \chi_1^2(1) + \chi_2^2(1) + \sum_{i=3}^{\frac{n+3}{2}} \chi_i^2(1) \geq 2 \times 1 + \left(\frac{n+3}{2} - 3 + 1\right) \times 2^2 = 2n,$$

whence $\chi_i(1) = 2$ for all $3 \leq i \leq \frac{n+3}{2}$. Furthermore, as a consequence of Frobenius-Schur Theorem (see [Isa94, Corollary 4.6]), we have

$$n + 1 = \sum_{i=1}^{\frac{n+3}{2}} \nu_2(\chi_i)\chi_i(1),$$

where $\nu_2(\chi) \in \{-1, 0, 1\}$ for all $\chi \in \mathrm{Irr}(G)$. Hence,

$$n + 1 \leq \sum_{i=1}^{\frac{n+3}{2}} \chi_i(1) = 2 \times 1 + \left(\frac{n+3}{2} - 3 + 1\right) \times 2 = n + 1,$$

whence $\nu_2(\chi_i) = 1$ for all $1 \le i \le \frac{n+3}{2}$. By [Isa94, Corollary 4.19], this means that all irreducible characters of G are real-valued and afforded by real representations. We have just shown the remarkable result regarding irreducible characters of D_{2n} where n is odd:

Lemma 7. *If n is odd, then the set of irreducible characters of D_{2n} consists of 2 linear characters and $\frac{n-1}{2}$ characters of degree 2. Furthermore, all of them are real-valued and afforded by real representations.*

Now let χ be a non-linear irreducible character of G. We will show that $\chi(x) = 0$. Indeed, as x has order 2, $\chi(x) \in \{-1-1, -1+1, 1+1\} = \{-2, 0, 2\}$. However, if $|\chi(x)| = 2$, then $x^G \subset Z(\chi)$ and $2n = |G| = \sum_{g\in G} |\chi(g)|^2 \ge \sum_{g\in x^G} |\chi(g)|^2 = \sum_{g\in x^G} |\chi(x)|^2 = 2^2 \cdot |x^G| = 4n$, a contradiction! Therefore, $\chi(x) = 0$. Put $\varepsilon = e^{\frac{2\pi i}{n}}$. Because z has order n, $\chi(z)$ equals the sum of two n-th roots of unity, so there exists $1 \le p \le q \le n$ such that $\chi(z) = \varepsilon^p + \varepsilon^q$. Moreover, the fact that χ is real-valued yields $\varepsilon^p + \varepsilon^q \in \mathbb{R}$, which only happens when $0 = \sin\left(\frac{2p\pi}{n}\right) + \sin\left(\frac{2q\pi}{n}\right) = 2\sin\left(\frac{(p+q)\pi}{n}\right)\cos\left(\frac{(q-p)\pi}{n}\right)$ or equivalently, when one of the following conditions holds: $p+q = 2n$, or $p+q = n$, or $q - p = \frac{n}{2}$. However, $q - p \ne \frac{n}{2}$ because n is odd and $q-p \in \mathbb{Z}$. Besides, if $p+q = 2n$, then $p = q = n$ and $\chi(z) = \varepsilon^n + \varepsilon^n = 2$, resulting in $z \in \ker\chi$, so $\langle z\rangle \subset \ker\chi$. Once again, this leads to a contradiction because $2n = |G| = \sum_{g\in G} |\chi(g)|^2 \ge \sum_{g\in\langle x\rangle} |\chi(g)|^2 = 2^2 \cdot |\langle z\rangle| = 4n$. We deduce that $p + q = n$ and thus, $\chi(z) = \varepsilon^p + \varepsilon^{n-p} = \varepsilon^p + \varepsilon^{-p}$. Consequently, $\chi(z^j) = \varepsilon^{pj} + \varepsilon^{-pj}$ for all $1 \le j \le n-1$. In conclusion, χ must satisfy $\chi(x) = 0$ and $\chi(z^j) = e^{\frac{2pj\pi i}{n}} + e^{\frac{-2pj\pi i}{n}}$ for all values j and some $1 \le p \le \frac{n-1}{2}$. Because there are precisely $\frac{n-1}{2}$ non-linear irreducible characters of G, the above assertion has determined all of them. Therefore, the character table of D_{2n} where n is odd is given as shown:

D_{2n} (n odd)	1	z	$\cdots$	$z^{\frac{n-1}{2}}$	x
χ_1	1	1	$\cdots$	1	1
χ_2	1	1	$\cdots$	1	-1
χ_3	2	$e^{\frac{2\pi i}{n}} + e^{\frac{-2\pi i}{n}}$	$\cdots$	$e^{\frac{2(\frac{n-1}{2})\pi i}{n}} + e^{\frac{-2(\frac{n-1}{2})\pi i}{n}}$	0
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
$\chi_{\frac{n+3}{2}}$	2	$e^{\frac{2(\frac{n-1}{2})\pi i}{n}} + e^{\frac{-2(\frac{n-1}{2})\pi i}{n}}$	$\cdots$	$e^{\frac{2(\frac{n-1}{2})(\frac{n-1}{2})\pi i}{n}} + e^{\frac{-2(\frac{n-1}{2})(\frac{n-1}{2})\pi i}{n}}$	0

Now consider the remaining case when n is even. In this case, all irreducible characters of D_{2n} can be found through an analogous procedure. Because the process is pretty similar to what have just been done, we only state the main steps without detailed verification:

- If n is even, there are precisely $\frac{n}{2} + 3$ conjugacy classes of D_{2n} which are:
$$\{1\}, \{z^{\frac{n}{2}}\}, \{z, z^{n-1}\}, \ldots, \{z^{\frac{n}{2}-1}, z^{\frac{n}{2}+1}\}, \text{ and}$$
$$\left\{z^{2j}x : 0 \le j \le \frac{n}{2} - 1\right\}, \left\{z^{2j+1}x : 0 \le j \le \frac{n}{2} - 1\right\}.$$
Consequently, there are precisely $\frac{n}{2} + 3$ irreducible characters of D_{2n}.
- It is routine to check that $D'_{2n} \cong \mathbb{Z}_{\frac{n}{2}}$. As a result, there are $[D_{2n} : D'_{2n}] = 4$ linear characters of D_{2n}. Since $\chi(x), \chi(z) \in \{1, -1\}$ for all $\chi \in \mathrm{Irr}(G)$ satisfying $\chi(1) = 1$, we can deduce all linear characters defined as:
$$\chi_1 = 1_G, \quad \chi_2(z^i x^j) = (-1)^j, \quad \chi_3(z^i x^j) = (-1)^i, \quad \chi_4(z^i x^j) = (-1)^{i+j}.$$
- The equations $|G| = \sum_{\chi\in\mathrm{Irr}(G)} \chi^2(1)$ and $2 + n = \sum_{\chi\in\mathrm{Irr}(G)} \nu_2(\chi)\chi(1)$ indicate that all non-linear irreducible characters of G have degree 2 and moreover, they are real-valued.

- The non-linear irreducible characters are determined as follows:
$$\begin{cases} \chi(x) = \chi(zx) = 0, \text{ and} \\ \chi(z^j) = e^{pj\frac{2\pi i}{n}} + e^{-pj\frac{2\pi i}{n}} \text{ for some } 1 \le p \le \frac{n}{2} - 1. \end{cases}$$

Finally, we accomplish the table of D_{2n} where n is even:

D_{2n} (n even)	1	z	$\cdots$	$z^{\frac{n}{2}}$	x	zx
χ_1	1	1	$\cdots$	1	1	1
χ_2	1	1	$\cdots$	1	-1	-1
χ_3	1	-1	$\cdots$	$(-1)^{\frac{n}{2}}$	1	-1
χ_4	1	-1	$\cdots$	$(-1)^{\frac{n}{2}}$	-1	1
χ_5	2	$e^{\frac{2\pi i}{n}} + e^{-\frac{2\pi i}{n}}$	$\cdots$	-2	0	0
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	
$\chi_{\frac{n}{2}+3}$	2	$e^{\frac{2(\frac{n}{2}-1)\pi i}{n}} + e^{\frac{-2(\frac{n}{2}-1)\pi i}{n}}$	$\cdots$	$2(-1)^{\frac{n}{2}-1}$	0	0

□

4.5. Let g be an element of order n in a finite group G. Suppose g is a product of two squares in G and k is coprime to n. Show that g^k is also a product of two squares in G.

Solution. Our aim is to show a criterion to determine whether an element of a group is a product of two squares. To begin with, we start with a simple remark:

Lemma 8. *Let G be a finite group, $g \in G$. Then $g = a^2b^2$ for some $a, b \in G$ if and only if $g = cd^{-1}cd$ for some $c, d \in G$.*

Proof of Lemma 8. The assertions is straightforward from the following identities:
$$a^2b^2 = (a^2ba^{-1})(aba^{-1})(a^2ba^{-1})(aba^{-1})^{-1}, \text{ and}$$
$$cd^{-1}cd = (cd^{-1}c^{-1})^2(cd)^2.$$
□

Lemma 9. *Let G be a finite group, $g \in G$. Then $g = a^2b^2$ for some $a, b \in G$ if and only if*
$$\sum_{\chi \in Irr(G), \chi = \overline{\chi}} \frac{\chi(g)}{\chi(1)} \neq 0.$$

Proof of Lemma 9. We use the same notions as in Problem 3.6. Assume $g = a^2b^2$ for some $a, b \in G$, by Lemma 8, $g = cd^{-1}cd$ for some $c, d \in G$. Recall that
$$a_{ijv} = \frac{|\mathcal{K}_i||\mathcal{K}_j|}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g_i)\chi(g_j)\overline{\chi(g_v)}}{\chi(1)}$$
is a nonnegative integer for all triples (i, j, v). Let $\mathcal{K}_v$ is the conjugacy class containing g. Since c and $d^{-1}cd$ are in a common conjugacy class $\mathcal{K}_i$ for some i, we have $a_{iiv} > 0$, or equivalently
$$\sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(c)^2\overline{\chi(g)}}{\chi(1)} > 0.$$
On the other hand, because a_{ijv} is nonnegative for all triples (i, j, v), the following inequality holds as well:
$$\sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(h)^2\overline{\chi(g)}}{\chi(1)} \geq 0,$$

for all $h \in G$. Taking the sum of all the terms of the form in the left-hand side of the above inequality with respect to h over G, emphasizing that the term with respect to c is strictly larger than 0, we obtain that

$$\begin{aligned} 0 &< \sum_{h\in G}\sum_{\chi\in\mathrm{Irr}(G)} \frac{\chi(h)^2\overline{\chi(g)}}{\chi(1)} \\ &= \sum_{\chi\in\mathrm{Irr}(G)} \frac{\overline{\chi(g)}}{\chi(1)} \sum_{h\in G}\chi(h)^2 \\ &= |G| \sum_{\chi\in\mathrm{Irr}(G)} \frac{\overline{\chi(g)}}{\chi(1)}\langle \chi, \overline{\chi}\rangle \\ &= |G| \sum_{\chi\in\mathrm{Irr}(G);\chi=\overline{\chi}} \frac{\overline{\chi(g)}}{\chi(1)}, \end{aligned}$$

which can be simplified to our desired condition. Conversely, assume that

$$\sum_{\chi\in\mathrm{Irr}(G);\chi=\overline{\chi}} \frac{\chi(g)}{\chi(1)} \neq 0,$$

which means that

$$\sum_{h\in G}\sum_{\chi\in\mathrm{Irr}(G)} \frac{\chi(h)^2\overline{\chi(g)}}{\chi(1)} = |G| \sum_{\chi\in\mathrm{Irr}(G);\chi=\overline{\chi}} \frac{\chi(g)}{\chi(1)} \neq 0$$

as above equalities. By the aforementioned remark that $\sum_{\chi\in\mathrm{Irr}(G)} \frac{\chi(h)^2\overline{\chi(g)}}{\chi(1)} \geq 0$ for all $h \in G$, there is some $c \in G$ such that

$$\sum_{\chi\in\mathrm{Irr}(G)} \frac{\chi(c)^2\overline{\chi(g)}}{\chi(1)} > 0.$$

Hence, $a_{iiv} = \frac{|\mathcal{K}_i||\mathcal{K}_i|}{|G|}\sum_{\chi\in\mathrm{Irr}(G)} \frac{\chi(c)\chi(c)\overline{\chi(g)}}{\chi(1)} > 0$ where $c \in \mathcal{K}_i$ and $g \in \mathcal{K}_v$. From this we see $g = c \cdot c^d = c(d^{-1}cd)$ for some $d \in G$, or g can be written as a product of two squares in G by Lemma 6. The proof is complete. □

Back to the main problem, it is equivalent by Lemma 9 to prove that

$$\sum_{\chi\in\mathrm{Irr}(G);\chi=\overline{\chi}} \frac{\chi(g^k)}{\chi(1)} \neq 0,$$

provided that

$$\sum_{\chi\in\mathrm{Irr}(G);\chi=\overline{\chi}} \frac{\chi(g)}{\chi(1)} \neq 0,$$

from which the process is completely analogous to what we have done in Problem 3.6. □

4.6. Let $J = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}$. The symplectic group $S = Sp_{2n}(\mathbb{R})$ is defined to be the set of all $2n\times 2n$-matrices A over $\mathbb{R}$ such that ${}^tAJA = J$. Suppose a finite group G has a representation $\Phi : G \to S$, with character χ. Prove that the complex character χ cannot be irreducible.

Solution. Assume by contradiction that the complex character χ is irreducible. Since ${}^t\Phi(g)J\Phi(g) = J$ for all $g \in G$, it follows that ${}^tJ = \vartheta_2(\chi)J$ (see [Isa94, Theorem 4.14]), from which it implies that $\vartheta_2(\chi) = -1$ as ${}^tJ = -J$ by setting. On the other hand, [Isa94, Corollary 4.15] says that $\vartheta_2(\chi) = 1$, which is a contradiction. Hence χ cannot be irreducible. □

4.7. Let G be a simple group and let $S \in \mathrm{Syl}_2(G)$ be a proper elementary abelian of order $q = 2^f$. Suppose $S = C_G(x)$ for any x, $1 \neq x \in S$. Prove the following statements.

(a) Any 2-element of G is conjugate to an element of S. If $g \in G$, then either g is an involution, or g has odd order.
(b) Let x be an involution in S. Then G has at least one involution $y \notin S$. Moreover, x and y are conjugate in G.
(c) Using (b), show that G has exactly $\frac{|G|}{q}$ involutions, and they are all conjugate.
(d) $\vartheta_2(\chi) = 1$ for all $\chi \in \mathrm{Irr}(G)$. If $\chi \in \mathrm{Irr}(G)$ and $\chi \neq 1_G$, and x any involution, then $\chi(x) = \chi(1) - q$.

Proof. The following result is quite ordinary but it is necessary to state for it would have been used for several times.

Lemma 10. *With the same assumptions as above, if T is any other 2-Sylow subgroup, then T is an elementary abelian group of order $q = 2^f$ and $T = C_G(t)$ for all $1 \neq t \in T$ as well.*

Proof of Lemma 10. If $T \in \mathrm{Syl}_2(G)$, then, according to Sylow's Theorem, there exists $h \in G$ such that $T^h = S$. From this we see it is quite clear that T is also an elementary abelian group of order q. As a consequence, $T \subseteq C_G(t)$ for all $t \in T$. It remains to show that $C_G(t) \subseteq T$ if $t \in T \setminus \{1\}$. Indeed, for any $k \in C_G(t)$, $k^h t^h = (kt)^h = (tk)^h = t^h k^h$. Because $1 \neq t^h \in S$, so $k^h \in C_G(t^h) = S$, it means that $k \in S^{h^{-1}} = T$. Thus, $T = C_G(t)$ for all $t \in T \setminus \{1\}$. □

(a) Let $t \in G$ be a 2-element of G. By Sylow's Theorems, there is a subgroup $T \in \mathrm{Syl}_2(G)$ containing t such that $T = S^h$ for some $h \in G$, and so our first assertion holds. Next, we shall show that every element of even order is an involution. Indeed, for any $g \in G$ of even order $2^k n$, where $k \geq 1$ and n is odd, g^n is a 2-element in G. It is derived from the first assertion that $g^n \neq 1$, contained in a 2-Sylow subgroup T, is conjugate to an element of S, so g^n is an involution, or it means that $k = 1$. By Lemma 10, $g^2 \in C_G(g^n) = T$, which leads to $n = \left|g^2\right| \mid |T| = 2^f$. Thus $n = 1$ as n is odd. In conclusion, g is an involution.
(b) Because G is a simple group, there exists an element $h \in G$ such that $S^h \nsubseteq S$. Therefore, there exists an element $y \in S^h \setminus S$. In addition, y is an involution by Lemma 10.
Assume by contradiction that there exists an involution $y \notin S$ not conjugate to x. If $(xy)^2 = 1$, then $xy = yx$, which implies $y \in C_G(x) = S$, a contradiction! Thus $|xy| > 2$. By assumption, the order of xy must be even since if otherwise, it contradicts to what have been stated in Problem 4.4(a). In addition, $Z(\langle x, y\rangle) = \left\{1, (xy)^{\frac{|xy|}{2}}\right\}$, according to Problem 4.4(b). In particular, x and y both commute to the involution $(xy)^{\frac{|xy|}{2}}$. Therefore $(xy)^{\frac{|xy|}{2}} \in C_G(x) \setminus \{1\} = S \setminus \{1\}$, so $y \in C_G((xy)^{\frac{|xy|}{2}}) = S$. This is a contradiction!
(c) Let y be another involution in G. If $y \notin S$, y is conjugate to x by part (b). Otherwise, y and x are both conjugate to a common involution not in S. Hence they are conjugate to each other. To sum up, all involutions in G are conjugate to x. Conversely, it is obvious that any element conjugate to x is an involution. Therefore, the number of involutions in G is equal to $\left|x^G\right| = [G : C_G(x)] = \frac{|G|}{|S|} = \frac{|G|}{q}$.
(d) It is obvious that $\vartheta_2(1_G) = 1$. Let x be any involution in G, by Lemma 10, the roles of all 2-Sylow subgroup are interchangeable, so we can assume that $x \in S$. Pick $\chi \in \mathrm{Irr}(G) \setminus \{1_G\}$. χ_S is real for $\overline{\chi(y)} = \chi(y^{-1}) = \chi(y)$ for every $y \in S$. According to (c), $\chi(y) = \chi(x)$ for all

$1 \neq y \in S$. We obtain that

$$\begin{aligned}
\langle \chi_S, 1_S \rangle &= \frac{1}{|S|} \sum_{y \in S} \chi_S(y) 1_S(y) \\
&= \frac{1}{q} \sum_{y \in S} \chi(y) \\
&= \frac{1}{q} \left(\chi(1) + \sum_{1 \neq y \in S} \chi(y) \right) \\
&= \frac{1}{q} \left(\chi(1) + (q-1)\chi(x) \right) \\
&= \frac{1}{q} (\chi(1) - \chi(x)) + \chi(x) \in \mathbb{Z}.
\end{aligned}$$

Therefore, $\chi(x) \in \mathbb{Q}$. In addition, $\chi(x)$ is an algebraic integer (see [Isa94, Corollary 3.6]), so $\chi(x) \in \mathbb{Z}$ by [Isa94, Lemma 3.2]. According the above equatilies, $q \mid \chi(1) - \chi(x)$. We claim that $\chi(1) - \chi(x) = q$. Indeed, we complete the claim through the following steps:

Firstly, observe that $\chi(1) \geq |\chi(x)| \geq \chi(x)$. Because G is a simple group, $\ker \chi$ is equal to either 1 or G. However, if $\ker \chi = G$, then $\chi = \chi(1) 1_G$, so $\chi(1) = 1$ and $\chi = 1_G$, a contradiction! Thus $\ker \chi = 1$, which combining with the observation leads to $\chi(1) > \chi(x)$. As $q \mid \chi(1) - \chi(x)$, it follows that $\chi(x) \leq \chi(1) - q$.

Secondly, as x and 1 are not conjugate, [Isa94, Theorem 2.18] states that

$$\begin{aligned}
0 &= \sum_{\chi \in \mathrm{Irr}(G)} \chi(x) \overline{\chi(1)} \\
&= 1_G(x) 1_G(1) + \sum_{\chi \in \mathrm{Irr}(G) \backslash \{1_G\}} \chi(x) \chi(1) \\
&\leq 1 + \sum_{\chi \in \mathrm{Irr}(G) \backslash \{1_G\}} (\chi(1) - q) \chi(1) \\
&= 1 + \sum_{\chi \in \mathrm{Irr}(G) \backslash \{1_G\}} \chi^2(1) - q \left(\sum_{\chi \in \mathrm{Irr}(G) \backslash \{1_G\}} \chi(1) \right) \\
&= |G| - q \left(\sum_{\chi \in \mathrm{Irr}(G) \backslash \{1_G\}} \chi(1) \right).
\end{aligned}$$

Therefore,

$$\sum_{\chi \in \mathrm{Irr}(G) \backslash \{1_G\}} \chi(1) \leq \frac{|G|}{q}.$$

Finally, according to [Isa94, Corollary 4.6] and part (c),

$$\begin{aligned}1+\frac{|G|}{q} &= \sum_{\chi\in\mathrm{Irr}(G)} \vartheta_2(\chi)\chi(1)\\ &= \vartheta_2(1_G)1_G(1) + \sum_{\chi\in\mathrm{Irr}(G)\setminus\{1_G\}} \vartheta_2(\chi)\chi(1)\\ &\leq 1 + \sum_{\chi\in\mathrm{Irr}(G)\setminus\{1_G\}} \chi(1)\\ &\leq 1+\frac{|G|}{q}.\end{aligned}$$

This occurs if and only if $\vartheta_2(\chi)=1$ and $\chi(1)-q=\chi(x)$ for all $\chi\in\mathrm{Irr}(G)$. The proof is complete.

□

5.1. For any finite group X, set $b(X)=\max\{\chi(1):\chi\in\mathrm{Irr}(X)\}$. If H is a subgroup of G, show that $b(H)\leq b(G)\leq [G:H]b(H)$.

Solution. Let ϑ be an arbitrary irreducible character of H. Then, [Isa94, Corollary 5.4] asserts the existence of an irreducible character χ of G such that ϑ is a constituent of χ_H. Hence, $\vartheta(1)\leq\chi_H(1)=\chi(1)\leq b(G)$ and thus, $b(H)\leq b(G)$. Now let ρ be an arbitrary irreducible character of G. Then, ρ_H is a character of H, we let $\lambda\in\mathrm{Irr}(H)$ denote one of its constituents. It follows from Frobenius reciprocity that $\langle\rho,\lambda^G\rangle_G=\langle\rho_H,\lambda\rangle_H>0$, i.e. ρ is a constituent of the induced character λ^G, so $\rho(1)\leq\lambda^G(1)=[G:H]\lambda(1)\leq[G:H]b(H)$, meaning that $b(G)\leq[G:H]b(H)$ and we deduce the desired inequalities. □

5.2. Let χ be a monomial character of a finite group G and suppose K is a subgroup of G such that $\chi_K\in\mathrm{Irr}(K)$. Show that χ_K is a monomial character of K.

Solution. By assumption, there exist a subgroup H of G and a linear character $\lambda\in\mathrm{Irr}(H)$ such that $\chi=\lambda^G$ and moreover, $(\lambda^G)_K=\chi_K\in\mathrm{Irr}(K)$. Denote by $[H\backslash G/K]$ the set of (H,K)-double coset representatives, it means that $G=\bigsqcup_{t\in[H\backslash G/K]}HtK$. Applying Mackey's Formula, we have

$$(\lambda^G)_K=\sum_{t\in[H\backslash G/K]}((\lambda_{H\cap K^t})^{t^{-1}})^K.$$

Because $(\lambda^G)_K$ is an irreducible character, the above formula implies that $|[H\backslash G/K]|=1$ and $G=HK$. Also, the formula indicates that $\chi_K=(\lambda^G)_K=(\lambda_{H\cap K})^K$, where $\lambda_{H\cap K}$ is a linear character of $H\cap K$. In conclusion, $\chi_K=(\lambda_{H\cap K})^K$ is a monomial character of K. □

5.3. Consider the character table C of a finite group G. Show that the sum of all entries of any row is a non-negative rational integer. Also, show that $|\det(C)|^2$ is a positive integer if we view C as a matrix.

Solution. Let G act on G via conjugation. Suppose that there are precisely k conjugacy classes in G and $\{g_1,\dots,g_k\}$ is the complete set of representatives of these conjugacy classes. We will first show that the sum of entries of any row of the character table of G is a non-negative rational integer, which is equivalent to saying that $\sum_{i=1}^k\chi(g_i)\in\mathbb{N}\cup\{0\}$ for all $\chi\in\mathrm{Irr}(G)$. Consider the permutation character ϑ on G of the aforementioned action, which is defined as

$$\vartheta(g)=|\{h\in G:h^g=h\}|=|\{h\in G:hg=gh\}|=\frac{|G|}{|\mathrm{Cl}(g)|}.$$

Therefore,

$$\begin{aligned}\sum_{i=1}^{k}\chi(g_i) &= \sum_{i=1}^{k}\sum_{g\in \mathrm{Cl}(g_i)}\frac{\chi(g)}{|\mathrm{Cl}(g_i)|}\\ &= \sum_{g\in G}\frac{\chi(g)}{|\mathrm{Cl}(g)|}\\ &= \frac{1}{|G|}\sum_{g\in G}\chi(g)\frac{|G|}{|\mathrm{Cl}(g)|}\\ &= \frac{1}{|G|}\sum_{g\in G}\chi(g)\overline{\vartheta(g)}\\ &= \langle \chi,\vartheta\rangle \in \mathbb{N}\cup\{0\},\end{aligned}$$

which finishes the first assertion. Also, if we denote $\mathrm{Irr}(G)=\{\chi_1,\ldots,\chi_k\}$ and we view C as a $k\times k$ matrix where $C_{ij}=\chi_i(g_j)$, then

$$|\det(C)|^2 = \overline{\det C}\ \det C = \det\overline{C}\det C = \det({}^t\overline{C}C).$$

We already know from [Isa94, Theorem 2.18] that ${}^t\overline{C}C$ is a $k\times k$ diagonal matrix whose (i,i)-th entry is $\frac{|G|}{|\mathrm{Cl}(g_i)|}=\vartheta(g_i)$. Therefore, $|\det(C)|^2=\det({}^t\overline{C}C)=\prod_{i=1}^{k}\vartheta(g_i)$, a positive integer, and the proof is complete. □

5.4. Let G act doubly transitively on a finite set Ω. Let $\alpha,\beta\in\Omega$ with $\alpha\neq\beta$. Denote $H=\mathrm{Stab}_G(\alpha)$, $K=\mathrm{Stab}_G(\alpha)\cap\mathrm{Stab}_G(\beta)$. Suppose $\phi\in\mathrm{Irr}(H)$ and $\phi_K\in\mathrm{Irr}(K)$. Show that $\langle\phi^G,\phi^G\rangle_G\leq 2$.

Solution. Assume by contradiction that $\langle\phi^G,\phi^G\rangle_G\geq 3$. Because G acts transitively on the Ω, there exists an element $t\in G$ such that $\alpha^t=\beta$.

Firstly, we claim that G is a disjoint union of two (H,H)-double cosets, that is, $G=H\sqcup Ht^{-1}H$. Indeed, for any $g\in G\backslash H=G\backslash\mathrm{Stab}_G(\alpha)$, we have $\alpha^{g^{-1}}\neq\alpha$. Since G acts doubly, $\alpha^{g^{-1}}$ and β belong to a common orbit other than $\{\alpha\}$ under the action of H, it means that there exists an element $h\in H$ such that $\alpha^{g^{-1}h}=(\alpha^{g^{-1}})^h=\beta=\alpha^t$. Thus, $\alpha^{g^{-1}ht^{-1}}=\alpha$, so $g^{-1}ht^{-1}\in\mathrm{Stab}_G(\alpha)=H$, or equivalently $g\in Ht^{-1}H$. On the other hand, the union is disjoint as $H\cap Ht^{-1}H=\emptyset$ from the fact that $t^{-1}\notin H$.

Secondly, we have

$$\begin{aligned}\mathrm{Stab}_G(\beta) &= \{g\in G:\beta^g=\beta\}\\ &= \{g\in G:\alpha^{tg}=\alpha^t\}\\ &= \{g\in G:\alpha^{tgt^{-1}}=\alpha\}\\ &= \{g\in G: tgt^{-1}\in H\}\\ &= t^{-1}Ht\\ &= H^t,\end{aligned}$$

so $K=H\cap H^t$. According to Mackey's Formula,

$$\begin{aligned}\left(\phi^G\right)_H &= \left(\phi_{H\cap H^1}\right)^{1^{-1}}\Big)^H + ((\phi_{H\cap H^{t^{-1}}})^t)^H\\ &= \phi + ((\phi_{H\cap H^{t^{-1}}})^t)^H.\end{aligned}$$

Finally, Frobenius Reciprocity gives us another way of computing $\langle \phi^G, \phi^G \rangle_G$:

$$\begin{aligned}\langle \phi^G, \phi^G \rangle_G &= \left\langle \phi, (\phi^G)_H \right\rangle_H \\ &= \langle \phi, \phi \rangle_H + \left\langle \phi, ((\phi_{H \cap H^{t^{-1}}})^t)^H \right\rangle_H \\ &= \langle \phi, \phi \rangle_H + \langle \phi, ((\phi_{K^{t^{-1}}})^t)^H \rangle_H \\ &= 1 + \langle \phi_K, (\phi_{K^{t^{-1}}})^t \rangle_K.\end{aligned}$$

From the assumption, we derive that $\left\langle \phi_K, (\phi_{K^{t^{-1}}})^t \right\rangle \geq 2$. Thus,

$$2\phi(1) = 2\phi_K(1) \leq (\phi_{K^{t^{-1}}})^t(1) = \phi(1),$$

from which we gain a contradiction! We conclude that $\langle \phi^G, \phi^G \rangle_G \leq 2$. The proof is complete. $\square$

5.5. For any $\chi \in \mathcal{C}(G)$, set $\chi^{(n)}(g) = \chi(g^n)$. Suppose $G = H \times A$ with A abelian and $(|H|, n) = 1$. Show that $\chi^{(n)} \in \operatorname{Irr}(G)$ for all $\chi \in \operatorname{Irr}(G)$.

Solution. Let $\chi \in \operatorname{Irr}(G)$. According to [Isa94, Theorem 4.21], $\chi = \phi \times \theta$ where $\phi \in \operatorname{Irr}(H)$ and $\theta \in \operatorname{Irr}(A)$. It is routine to check that $\phi^{(n)} \in \mathcal{C}(H)$ and $\theta^{(n)} \in \mathcal{C}(A)$.

Firstly, we claim that $\phi^{(n)} \in \operatorname{Irr}(H)$. Because $(n, |H|) = 1$, the map transforming each element of H into the its n-th power is a bijection from H into itself, or equivalently $H = \{h^n : h \in H\}$. We have

$$\begin{aligned}\langle \phi^{(n)}, \phi^{(n)} \rangle &= \frac{1}{|H|} \sum_{h \in H} \left| \phi^{(n)}(h) \right|^2 \\ &= \frac{1}{|H|} \sum_{h \in H} |\phi(h^n)|^2 \\ &= \frac{1}{|H|} \sum_{h \in H} |\phi(h)|^2 \\ &= \langle \phi, \phi \rangle \\ &= 1.\end{aligned}$$

On the other hand, according to [Isa94, Problem 4.7], $\phi^{(n)}$ is a difference of characters of H, which is generally a $\mathbb{Z}$-linear combination of irreducible characters of H. Combining with the fact that $\langle \phi^{(n)}, \phi^{(n)} \rangle = 1$, $\phi^{(n)}$ must be either equal to some irreducible character or minus of some irreducible character of H. Nonetheless, the latter occurrence cannot happen since $\phi^{(n)}(1) = \phi(1) > 0$, so $\phi^{(n)} \in \operatorname{Irr}(H)$. The claim is proved.

Next, we also claim that $\theta^{(n)} \in \operatorname{Irr}(A)$. Since A is abelian, $\theta^{(n)}(1) = \theta(1) = 1$. It is routine that $\theta^{(n)}(uv) = \theta^{(n)}(u)\theta^{(n)}(v)$ for all $u, v \in A$, which indicates that $\theta^{(n)}$ is a representation of degree one, or equivalently $\theta^{(n)} \in \operatorname{Irr}(A)$.

Finally, for all $h \in H$ and $a \in A$, we have that

$$\begin{aligned}\chi^{(n)}(h \cdot a) &= \chi((h \cdot a)^n) \\ &= \chi(h^n \cdot a^n) \\ &= \phi(h^n)\theta(a^n) \\ &= \phi^{(n)}(h)\theta^{(n)}(a).\end{aligned}$$

Thus $\chi^{(n)} = \phi^{(n)} \times \theta^{(n)}$. Because $\phi^{(n)} \in \operatorname{Irr}(H)$ and $\theta^{(n)} \in \operatorname{Irr}(A)$, $\chi^{(n)} \in \operatorname{Irr}(G)$ by [Isa94, Theorem 4.21]. The proof is complete. $\square$

5.6. Consider the permutation actions of the symmetric group $G = \operatorname{Sym}_n$, $n \geq 5$, on $\{1, 2, 3, \ldots, n\}$, respectively on the set of unordered pairs $\{i, j\}, 1 \leq i \neq j \leq n$, with permutation character α, respectively, β. Show that there are some irreducible characters χ_1 of dergee $n-1$ and χ_2 of degree $\frac{n(n-3)}{2}$ of G such that $\alpha = 1_G + \chi_1$ and $\beta = 1_G + \chi_1 + \chi_2$.

Solution. It is obvious G acts doubly transitively on the set $\{1, 2, 3, \ldots, n\}$ by [Isa94, Corollary 5.16]. According to [Isa94, Corollary 5.17], there exists an irreducible character $\chi_1 \in \mathrm{Irr}(G)$ such that $\alpha = 1_G + \chi_1$. In particular, $\chi_1(1) = \alpha(1) - 1_G(1) = n - 1$. Let $V = \bigoplus_{1\le i\neq j\le n} \mathbb{C}\{i, j\}$ be the $\mathbb{C}G$-module with the set of unordered pairs $\{i, j\}$ as a basis. It is clear that V corresponds to β. For the rest of the proof, our aim is first show the existence of a $\mathbb{C}G$-submodule W of V whose character is precisely α. Then, it remains to show that the character corresponding to the submodule W' in the decomposition (by Maschke's Theorem) $V = W \oplus W'$ is irreducible.

Let $v_i = \sum_{1\le j\le n; j\neq i}\{i, j\} \in V$ for each $1 \le i \le n$, and let W be the $\mathbb{C}$-space generated by $\{v_i\}_{i=1}^n$. Suppose that $\sum_{i=1}^n a_i v_i = 0$ for some $a_i \in \mathbb{C}$, or explicitly that

$$0 = \sum_{i=1}^{n} a_i \left(\sum_{1\le j\le n; j\neq i} \{i, j\} \right) = \sum_{1\le j\neq i\le n} (a_i + a_j)\{i, j\}.$$

The equality holds if and only if $a_i + a_j = 0$ for all pairs $1 \le j \neq i \le n$, and straightforwardly if and only if all the a_i's are identically zero. Thus, $\{v_i\}_{i=1}^n$ is linear independent. Moreover, W is invariant under the action of G, that is,

$$v_i g = \left(\sum_{1\le j\le n; j\neq i} \{i, j\} \right) g = \sum_{1\le j\le n; j\neq i} \{i^g, j^g\} = \sum_{1\le j\le n; j\neq i^g} \{i^g, j\} = v_{i^g}$$

for all $g \in G$, $1 \le i \le n$. It is enough to point out that α is in fact the character corresponding to W:

$$\begin{aligned}
\alpha(g) &= |\{i : i^g = i\}| \\
&= |\{v_i : i^g = i\}| \\
&= |\{v_i : v_{i^g} = v_i\}| \\
&= |\{v_i : v_i g = v_i\}|,
\end{aligned}$$

for all $g \in G$.

Finally, according to Maschke's Theorem [Isa94, Theorem 1.9], $V = W \oplus W'$ for some $\mathbb{C}G$-submodule W' of V. Denote by χ_2 the character corresponding to W'. As 1_G and χ_1 are two distinct irreducible consitudents of β (as they are of α), it suffices to assert the irreducibility of χ_2 by indicating $\langle \beta, \beta \rangle = 3$. It is prominent that if $n \ge 5$, $G = \mathrm{Sym}_n$ acts transitively on the set of unordered pairs $\{i, j\}$, where $1 \le i \neq j \le n$. By [Isa94, Corollary 5.16], it is enough to show that $\mathrm{Stab}_G(\{1, 2\}) = \{g \in G : \{1, 2\}^g = \{1, 2\}\}$ has exactly 3 orbits on the set of pairs $\{i, j\}$, $1 \le j \neq i \le n$. To show this, we shall show that $\{1, 2\}$, $\{1, 3\}$ and $\{4, 5\}$ are the representatives of all the orbits under the action of $\mathrm{Stab}_G(\{1, 2\})$. First, it is evident that the orbit of $\{1, 2\}$ contains a single element. For any $g \in \mathrm{Stab}_G(\{1, 2\})$, we have $\{1, 3\}^g = \{1^g, 3^g\} \neq \{4, 5\}$ as 1 is only moved to either 1 or 2, it means that $\{1, 3\}$ and $\{4, 5\}$ represent at least two orbits of $\mathrm{Stab}_G(\{1, 2\})$. In fact, they is no other orbit. Indeed, for any $\{i, j\} \neq \{1, 2\}$, we will prove that $\{i, j\}$ belongs to the orbit of either $\{1, 3\}$ or $\{4, 5\}$:

- If neither of these i and j is equal to 1 or 2, then $\{i, j\}$ belongs to the orbit containing $\{4, 5\}$ because $\{i, j\}^{(i\ 4)(j\ 5)} = \{4, 5\}$;
- if one of them is equal to 2, say $i = 2$, then $\{i, j\}$ belongs to orbit containing $\{1, 3\}$ as $\{i, j\}^{(2\ 1)(j\ 3)} = \{1, 3\}$;
- if one of them is equal to 1, say $i = 1$, then $\{i, j\}$ belongs to the orbit containing $\{1, 3\}$ since $\{i, j\}^{(j\ 3)} = \{1, 3\}$.

In conclusion, we see that $\beta = \alpha + \chi_2 = 1_G + \chi_1 + \chi_2$ where χ_1, χ_2 are irreducible and $\chi_1(1) = n-1$ and $\chi_2(1) = \frac{n(n-3)}{2}$. The proof is complete. $\square$

5.7. Let G be a simple group and let $S \in \mathrm{Syl}_2(G)$ be elementary abelian of order $q = 2^f$. Suppose $S = C_G(x)$ for any $x, 1 \neq x \in S$. Prove that $|G| = q(q+1)(q-1)$ following the steps below.

(a) Let $N = N_G(S)$. Show that N acts transitively on $q-1$ involutions of S, hence $|N| = q(q-1)$.
(b) Fix a $\lambda \in \mathrm{Irr}(N)$ with $\lambda \neq 1_N$ and $\ker \lambda \geq S$. Show that $\lambda^G(s) = \lambda(1)$ for all $s \in S, s \neq 1$.
(c) If $\chi \in \mathrm{Irr}(G)$ is a constituent of λ^G, then $\chi(1) \geq q+1$.
(d) Decompose $\lambda^G = \sum_\chi a_\chi \chi$ with $\chi \in \mathrm{Irr}(G)$, $a_\chi \geq 1$. Let $s \in S \setminus \{1\}$. By (c) and Problem 4.7-(d),

$$\lambda(1) = \lambda^G(s) = \sum_\chi a_\chi(\chi(1) - q) = [G : N]\lambda(1) - q\sum_\chi a_\chi,$$

hence $\sum_\chi a_\chi \leq \lambda(1)$. Using this inequality and the fact that $\lambda(1)$ divides $q-1 = [N : S]$, show that $[G : N] = q+1$. Consequently, $|G| = q(q^2-1)$.

Solution. (a) It is clear that the action of N by conjugation on $q-1$ involutions of S is well-defined. We shall prove that the action is transitive. Indeed, if $r, t \in S$ are arbitrary involutions of S, then, by Problem 4.7-(c), there exists an element $g \in G$ such that $r^g = t$. Remark that for every $s \in S = C_G(r)$, we have $s^g \in C_G(r^g) = C_G(t) = S$, which means $S^g = S$, or equivalently $g \in N_G(S) = N$. Thus, N acts transitively on $S \setminus \{1\}$. Lastly, by Orbit-Stabilize Theorem, for some $s \in S \setminus \{1\}$,

$$|N| = |N_s||S \setminus \{1\}| = |C_N(s)||S \setminus \{1\}| = |S|(|S| - 1) = q(q-1).$$

(b) Let s be a non-trivial element S. First, we state that all involutions of N belong to S. Indeed, if $n \in N$ is an involution, it follows that $(ns)^2 = (nsn)s \in S$ because $nsn = n^{-1}sn = s^n \in S$ as $n \in N = N_G(S)$. It implies that $(ns)^4 = \left((ns)^2\right)^2 = 1$, or that ns is of an even order. Thus ns is either 1 or an involution as stated in Problem 4.7-(a). Both situations asserts the statement since it means that $s = s^{-1} = nsn = s^n$, or equivalently that $n \in C_G(s) = S$. Then, let $t_1 = 1, t_2, \ldots, t_{[G:N]}$ be complete representatives of the right cosets N in G. We aim to show that $s^{t_i} \notin S$ when $2 \leq i \leq [G : N]$. Assume by contradiction that $s^{t_i} \in S$ for some index $2 \leq i \leq [G : N]$. By the transitivity of the action of N on $S \setminus \{1\}$, there is some element $z \in N$ such that $s^z = s^{t_i}$, which means that $t_i z^{-1} \in C_G(s) = S \subset N$, so $t_i \in N$, a contradiction! Thus S is not contained s^{t_i} for every $2 \leq i \leq [G : N]$, and neither is N since s^{t_i} is an involution by the first statement. Finally, as the definition of induced class function, we have

$$\lambda^G(s) = \frac{1}{|N|}\sum_{g \in G} \lambda^\circ(s^g) = \sum_{i=1}^{[G:N]} \lambda^\circ(s^{t_i}) = \lambda(s^{t_1}) = \lambda(s) = \lambda(1)$$

since $S \leq \ker \lambda$.

(c) Recall that there are characters $\hat{\lambda}$ and $\hat{\overline{\lambda}}$ of $N/\ker\lambda = N/\ker\overline{\lambda}$ defined as $\hat{\lambda}(\overline{g}) = \lambda(g)$ and $\hat{\overline{\lambda}}(\overline{g}) = \overline{\lambda}(g)$ for all $g \in G$. We have $[N : \ker\lambda]$ is odd since it divides $[G : S]$, which is an odd number. As a consequence, $\hat{\lambda}$ is different from $\overline{\hat{\lambda}} = \hat{\overline{\lambda}}$ as stated in Problem 3.2-(a), which leads to $\lambda \neq \overline{\lambda}$.

Note that χ is a real-valued character deduced from the fact that $\vartheta(\chi) = 1$ as stated in Problem 4.7-(d) and Frobenius-Schur Theorem. By Frobenius Reciprocity, we have

$$\langle \chi_N, \overline{\lambda} \rangle = \left\langle \chi, \overline{\lambda}^G \right\rangle = \left\langle \overline{\chi}, \overline{\lambda}^G \right\rangle = \left\langle \overline{\overline{\lambda}^G}, \chi \right\rangle = \langle \lambda^G, \chi \rangle > 0,$$

and

$$\langle \chi_N, \lambda \rangle = \langle \chi, \lambda^G \rangle > 0.$$

As a result, both λ and $\overline{\lambda}$ are constituents of χ_N, and hence so is $\lambda + \overline{\lambda}$. Hence, $(\lambda + \overline{\lambda})_S = \lambda_S + \overline{\lambda}_S = 2\lambda(1)1_S$ (as $S \leq \ker \lambda$) is a constituent of χ_S. Therefore

$$\begin{aligned}\langle \chi_S, 1_S \rangle &\geq \langle 2\lambda(1)1_S, 1_S \rangle \\ &= 2\lambda(1) \\ &\geq 2.\end{aligned}$$

On the other hand, according to Problem 4.7-(d),

$$\begin{aligned}\langle \chi_S, 1_S \rangle &= \frac{1}{|S|} \sum_{s \in S} \chi_S(s)\overline{1_S(s)} \\ &= \frac{1}{q} \sum_{s \in S} \chi(s) \\ &= \frac{1}{q} \left(\chi(1) + \sum_{s \in S \setminus \{1\}} \chi(s) \right) \\ &= \frac{1}{q} \left(\chi(1) + (q-1)(\chi(1) - q) \right) \\ &= \chi(1) - (q-1)\end{aligned}$$

Two ways of computing $\langle \chi_S, 1_S \rangle$ gives us the inequality $q + 1 \leq \chi(1)$ as desired.

(d) By (b) and Problem 4.7-(d), for $s \in S \setminus \{1\}$, we get that

$$\begin{aligned}\lambda(1) &= \lambda^G(s) \\ &= \sum_{\chi} a_\chi \chi(s) \\ &= \sum_{\chi} a_\chi (\chi(1) - q) \\ &= \sum_{\chi} a_\chi \chi(1) - q \sum_{\chi} a_\chi \\ &= \lambda^G(1) - q \sum_{\chi} a_\chi \\ &= [G : N]\lambda(1) - q \sum_{\chi} a_\chi.\end{aligned}$$

On the other hand, as mentioned in (c) that $\chi(1) \geq q + 1$,

$$\lambda(1) = \sum_{\chi} a_\chi (\chi(1) - q) \geq \sum_{\chi} a_\chi.$$

Therefore, we have

$$\begin{aligned}\lambda(1) &= [G : N]\lambda(1) - q \sum_{\chi} a_\chi \\ &\geq [G : N]\lambda(1) - q\lambda(1) \\ &= ([G : N] - q)\lambda(1),\end{aligned}$$

or equivalently

$$[G : N] \leq q + 1.$$

On the other side, famous Sylow's Theorem states that $[G : N] = [G : N_G(S)] = |\mathrm{Syl}_2(G)|$. Hence it is sufficient to show that $|\mathrm{Syl}_2(G)| \geq q + 1$. Equivalently, by picking a 2-Sylow subgroup P of G other than S (it always exists since if otherwise, $S \trianglelefteq G$, a contradiction), we claim that $\{P^s : s \in S\}$ is a collection of distinct 2-Sylow subgroups of G. Indeed, if there are $r \neq s$ as elements of S such that $P^r = P^s$. It means that $S^{gr} = S^{gs}$ for some element g of G by Sylow's Theorem, or equivalently that $S^{g(rs^{-1})g^{-1}} = S$. As a result, $g(rs^{-1})g^{-1} \in N_G(S) = N$. In addition, since $g(rs^{-1})g^{-1}$ is nontrivial and $\left(g(rs^{-1})g^{-1}\right)^2 = g(rs^{-1})^2 g^{-1} = 1$ for $rs^{-1} \in S$, it is an involution in N, hence in S as the first statement in the proof of part (b). Therefore,

$$1 \neq g(rs^{-1})g^{-1} \in S \cap S^{g^{-1}}.$$

According to Lemma 10, $S = C_G(grs^{-1}g^{-1}) = S^{g^{-1}}$, which implies $P = S^g = S$. A contradiction! Therefore, $\mathrm{Syl}_2(G)$ contains at least $q + 1$ elements including, for instance, S and P^s of G for all $s \in S$. In conclusion, $[G : N] = q + 1$ and consequently, we have

$$|G| = [G : N]|N| = (q + 1)q(q - 1).$$

Another approach of showing $[G : N] = q + 1$**:** Just like above, we have shown that $\lambda(1) \geq \sum_\chi a_\chi$ and

$$\lambda(1) = [G : N]\lambda(1) - q \sum_\chi a_\chi.$$

The latter equation can be rephrased into

$$\sum_\chi a_\chi = ([G : N] - 1)\lambda(1) - (q - 1) \sum_\chi a_\chi,$$

from which we obtain a new equation by dividing both sides by $\lambda(1)$:

$$\frac{\sum_\chi a_\chi}{\lambda(1)} = [G : N] - 1 - \frac{q - 1}{\lambda(1)} \sum_\chi a_\chi.$$

Here we note that $q - 1 = [N : S]$ is divisible by $\lambda(1)$ since

$$\lambda(1) = \hat{\lambda}(1) \mid |N/\ker\lambda| = [N : \ker\lambda] \mid [N : S] = q - 1.$$

Hence the left-hand side must be an integer. However, as $0 < \sum_\chi a_\chi \leq \lambda(1)$, this occurs if and only if $\sum_\chi a_\chi = \lambda(1)$, which means that $[G : N] = q + 1$.

$\square$

6.1. Let $N \triangleleft G$ and $\theta \in \mathrm{Irr}(N)$. Show that $\theta^G \in \mathrm{Irr}(G)$ if and only if $I_G(\theta) = N$.

Solution. Suppose that $\theta^G \in \mathrm{Irr}(G)$, and set $t = [G : I_G(\theta)]$ as the number of conjugates of θ. It is clear that $N \leq I_G(\theta)$. Using the Frobenius Reciprocity, we have

$$\langle \theta, (\theta^G)_N \rangle = \langle \theta^G, \theta^G \rangle = 1,$$

which deduces that θ is an irreducible constituent of $(\theta^G)_N$. By Clifford's Theorem (see [Isa94, Theorem 6.2]), we have

$$(\theta^G)_N = \langle \theta, (\theta^G)_N \rangle \left(\sum_{i=1}^t \theta_i \right) = \langle \theta^G, \theta^G \rangle \left(\sum_{i=1}^t \theta_i \right) = \sum_{i=1}^t \theta_i,$$

where the θ_i's are conjugates of θ. Thus,

$$[G : N]\theta(1) = \theta^G(1) = t\theta(1) = [G : I_G(\theta)]\theta(1).$$

Therefore, $|I_G(\theta)| = |N|$, or equivalently $I_G(\theta) = N$. Conversely, if $I_G(\theta) = N$, according to [Isa94, Theorem 6.11-(b)], $\theta^G \in \mathrm{Irr}(G)$. The proof is complete. $\square$

6.2. Let G be solvable and suppose that every $\chi \in \operatorname{Irr}(G)$ is quasiprimitive. Show that G is abelian.

Solution. Two following remarks are keys to solve the problem.

Lemma 11. *With the above assumption, every normal abelian subgroup of G is central.*

Proof of Lemma 11. Let K be a normal abelian subgroup of G. Since χ is quasiprimitive and K is abelian, χ_K is a multiple of a linear character. It is derived that $K \subseteq Z(\chi)$ for all $\chi \in \operatorname{Irr}(G)$. According to [Isa94, Corollary 2.28],

$$K \subseteq \bigcap_{\chi \in \operatorname{Irr}(G)} Z(\chi) = Z(G).$$

□

Lemma 12. *With the above assumption, every irreducible character of $G/Z(G)$ is quasiprimitive.*

Proof of Lemma 12. It is well-known that every normal subgroup of $G/Z(G)$ is of the form $K/Z(G)$ where $Z(G) \trianglelefteq K \trianglelefteq G$. Let $\hat{\chi}$ be an irreducible character of $G/Z(G)$. It is enough to show that $\hat{\chi}_{K/Z(G)}$ is a multiple of an irreducible character of $K/Z(G)$ for any subgroup K satisfying $Z(G) \trianglelefteq K \trianglelefteq G$. Indeed, [Isa94, Lemma 2.22] indicates that there is an irreducible character χ of G defined as $\chi(g) = \hat{\chi}(Z(G)g)$ for all $g \in G$. Since χ is quasiprimitive, $\chi_K = t\lambda$ for some irreducible character λ of G and $t \in \mathbb{N}$. By [Isa94, Lemma 2.21], $\ker \lambda = \ker \chi_K = \ker \chi \cap K \geq Z(G)$. Using again [Isa94, Lemma 2.22], we obtain the character $\hat{\lambda} \in \operatorname{Irr}(G/Z(G))$ defined as $\hat{\lambda}(Z(g)g) = \lambda(g)$ for all $g \in G$. We have

$$\begin{aligned}
\hat{\chi}_{K/Z(G)}(Z(G)k) &= \hat{\chi}(Z(G)k) \\
&= \chi(k) \\
&= t\lambda(k) \\
&= t\hat{\lambda}(Z(G)k),
\end{aligned}$$

for all $k \in K$, which means that $\hat{\chi}_{K/Z(G)} = t\hat{\lambda}$, a multiple of an irreducible character. In conclusion, $\hat{\chi}$ is quasiprimitive. □

We return to Problem 6.2. We will prove by strong induction on $k = |G|$ that G is abelian. It is clearly true for $k = 1$. Let $m \in \mathbb{N}$ be given and suppose that the assumption holds for all $1 \leq k \leq m$. Now we look at any group G of order $k = m + 1 \geq 2$. Since G is solvable, there is a positive integer n, called the derived length of G, such that n is the least positive integer such that the derived group $G^{(n)}$ is trivial. In particular, the $(n-1)$-th derived subgroup $G^{(n-1)}$ is non-trivial and abelian. Furthermore, it is clear that every subgroup of the commutator group $G' = G^{(1)}$ is normal in G, so is $G^{(n-1)}$. Applying Lemma 11, we get that $G^{(n-1)}$ is central, i.e. $G^{(n-1)} \leq Z(G)$. Consequently, $Z(G)$ is non-trivial, and so $|G/Z(G)| < |G|$. By the inductive assumption for $G/Z(G)$ and Lemma 12, we obtain that $G/Z(G)$ is abelian. If g is an arbitrary element of G, then $Z(G)\langle g \rangle / Z(G) \trianglelefteq G/Z(G)$ as $G/Z(G)$ is abelian, which is equivalent to $Z(G)\langle g \rangle \trianglelefteq G$. Moreover, one can verify that $Z(G)\langle g \rangle$ is abelian. By Lemma 11, $Z(G)\langle g \rangle \leq Z(G)$. In other words, we have $g \in Z(G)$. We conclude that G is abelian.

□

6.3a. Let $N \triangleleft G$ and suppose G/N is solvable. Let $\chi \in \operatorname{Irr}(G)$ and $\theta \in \operatorname{Irr}(N)$ with $\langle \chi_N, \theta \rangle_N > 0$. Show that $\chi(1)/\theta(1)$ divides $[G : N]$.

Solution. We begin with the remark that $\chi(1)/\theta(1)$ is an integer as stated in [Isa94, Lemma 6.8]. The statement is clearly true if $N = G$. Consider N as a proper subgroup of G. Recall that the equivalent definition of the solvability on non-trivial finite groups is a group with a composition series all of whose factors are cyclic groups of prime order. In other words, we have a composition series of length k

$$N/N = G_0/N \lhd \cdots \lhd G_k/N = G/N,$$

where each $(G_{i+1}/N)/(G_i/N) \simeq G_{i+1}/G_i$ is a cyclic group of prime order. We now prove by induction on the composition length k that $\chi(1)/\theta(1) \mid [G:N]$. For $k=1$, we have $[G:N]$ is a prime number. By applying [Isa94, Corolarry 6.19], then either $\chi_N = \theta$ or $\chi_N = \sum_{i=1}^{[G:N]} \theta^{a_i}$ where a_i's are elements of G, which implies that either $\chi(1) = \chi_N(1) = \theta(1)$ or $\chi(1) = \sum_{i=1}^{[G:N]} \theta^{a_i}(1) = [G:N]\theta(1)$. In either case, $\frac{\chi(1)}{\theta(1)}$ is an integer and divides $[G:N]$. Next, let $n \in \mathbb{N}$ be given and assume the statement holds for all $1 \le k \le n$. Consider a solvable group G/N whose composition length is $k = n+1$:

$$N/N = G_0/N \lhd \cdots \lhd G_{n+1}/N = G/N.$$

Notice that G_n/N and G/G_n are both solvable from the fact that G/N is solvable. On the other side, by Frobenius Reciprocity, we have $\langle \chi_{G_n}, \theta^{G_n} \rangle = \langle (\chi_{G_{n-1}})_N, \theta \rangle = \langle \chi_N, \theta \rangle > 0$. It means that there is an irreducible constituent $\phi \in \mathrm{Irr}(G_n)$ contained in both χ_{G_n} and θ^{G_n}. Applying the induction assumption on the solvable groups G/G_n, respectively, G_n/N of lengths 1, respectively, n, we gain that $\frac{\phi(1)}{\theta(1)} \mid [G_n:N]$ and $\frac{\chi(1)}{\phi(1)} \mid [G:G_n]$. Hence, we conclude that

$$\frac{\chi(1)}{\theta(1)} = \frac{\chi(1)}{\phi(1)} \frac{\phi(1)}{\theta(1)} \mid [G:G_n][G_n:N] = [G:N].$$

□

6.3. Suppose G has exactly one nonlinear irreducible character. Show that G' is an elementary abelian p-group (for a prime p). However, G is not always nilpotent.

Solution. We begin with a simple but powerful remark on the lower bound of the conjugacy classes of non-abelian finite group.

Lemma 13. *Every non-abelian finite group G has at least $[G:G']+1$ conjugacy classes where G' is its commutator subgroup. If G has precisely $[G:G']+1$ conjugacy classes, then every non-trivial element of G' is of order a fixed prime number.*

Proof of Lemma 13. Notice that G' is not trivial since G is non-abelian. It is clear that all the elements in a conjugacy class belongs to only one coset of G/G'. Moreover, each coset of G/G' contains at least one conjugacy class of G, where $G' \neq 1$ contains at least two which one of them is $1^G = \{1\}$. Therefore, there are at least $[G:G']+1$ conjugacy classes of G.

If G consists of $[G:G']+1$ conjugacy classes in total, then the coset G' consists of 2 while the other cosets have 1. As a result, all non-trivial elements of G' are conjugate to each other, which implies that they have a same order. Fix p as a prime divisor of $|G'|$. As G' is a non-trivial group, there exists an element of order p by Cauchy's Lemma. Therefore, all non-trivial elements of G' have the same order p as desired. □

A simple remark is that G is non-abelian as it has a nonlinear irreducible character, namely χ (see [Isa94, Corollary 2.6]). According to [Isa94, Corollary 2.23], the number of linear characters of G is equal to $[G:G']$. Therefore, the number of irreducible characters of G is $[G:G']+1$, so is the number of conjugacy classes of G by [Isa94, Corollary 2.7]. Applying Lemma 13, we have that every non-trivial element of G' is of order p for some prime number p.

In the rest of the solution, we shall prove that G' is abelian by showing that all irreducible characters of G' are linear characters. Assume by contradiction that there exists a nonlinear irreducible character λ of G'. For any irreducible constituent ϕ of λ^G, by Frobenius Reciprocity, we have $\langle \phi_{G'}, \lambda \rangle = \langle \phi, \lambda^G \rangle > 0$. Therefore, λ is an irreducible constituent of $\phi_{G'}$, which leads to $\phi(1) = \phi_{G'}(1) \ge \lambda(1) > 1$. As a result, the irreducible character ϕ must be equal to χ. It means that $\lambda^G = k\chi$ where $k = \langle \chi, \lambda^G \rangle = \langle \chi_{G'}, \lambda \rangle$. On the other hand, according to [Isa94, Theorem 6.2], we get that $\chi_{G'} = k \sum_{i=1}^t \lambda^{a_i}$ where a_i's are elements of G. To sum up, we obtain the following two identifications

$$k\chi(1) = \lambda^G(1) = \frac{|G|}{|G'|}\lambda(1); \text{ and } \chi(1) = \chi_{G'}(1) = k\sum_{i=1}^{t} \lambda_i(1) = kt\lambda(1).$$

Multiplying both identifications side by side and dividing by k, we obtain

$$\chi(1)^2 = \frac{t\lambda(1)^2|G|}{|G'|}.$$

Moreover, by [Isa94, Corollary 2.7], we have

$$\begin{aligned} |G| &= [G : G'] \times 1^2 + \chi(1)^2 \\ &= \frac{|G|}{|G'|} + \chi(1)^2 \\ &= \frac{|G|}{|G'|} + \frac{t\lambda(1)^2|G|}{|G'|} \\ &= \frac{|G|}{|G'|}\left(1 + t\lambda(1)^2\right), \end{aligned}$$

or equivalently,

$$\left|G'\right| - 1 = t\lambda(1)^2.$$

As a consequence, $\lambda(1) \mid |G'| - 1$. On the other hand, since $\lambda \in \mathrm{Irr}(G')$, we have $\lambda(1) \mid |G'|$ (see [Isa94, Theorem 3.11]). Therefore, $\lambda(1) = 1$, a contradiction! Thus, G' is abelian. To conclude, one can see that the symmetric group S_3 satisfies all of the conditions by the character table:

S_3	1	$(1\ 2\ 3)$	$(1\ 2)$
χ_1	1	1	1
χ_2	1	1	-1
χ_3	2	-1	0

Nonetheless, it is not nilpotent. $\square$

6.4. Let G be an M-group and suppose $N \triangleleft G$ with $(|N|, [G : N]) = 1$. Show that N is an M-group.

Solution. Recall that an M-group is a group whose all of the irreducible characters are monomial. Let $\theta \in \mathrm{Irr}(N)$ be an arbitrary irreducible character of N. Our main purpose is showing that θ is a monomial character. However, we shall initially show its conjugate being monomial, which indirectly declares our concern. To begin with, we fix λ^G, for some linear character $\lambda \in \mathrm{Irr}(H)$ for some $H \leq G$, as an irreducible constituent of θ^G. Put $M = NH$ and notice that it contains N. Therefore, we have $M^t \cap N = N$ for all $t \in G$ as $N \triangleleft G$. Denote by $[M \setminus G/N]$ the set of (M, N)-double coset representatives. Applying Mackey's Formula, we obtain that

$$(\theta^G)_M = \sum_{t \in [M\setminus G/N]} ((\theta_{M^t \cap N}))^{t^{-1}})^M = \sum_{t \in [M\setminus G/N]} (\theta^{t^{-1}})^M.$$

Then, as Frobenius Reciprocity, we deduce that

$$\begin{aligned}0 &< \langle \theta^G, \lambda^G \rangle \\ &= \langle \theta^G, (\lambda^M)^G \rangle \\ &= \langle (\theta^G)_M, \lambda^M \rangle \\ &= \left\langle \sum_{t \in [M \backslash G/N]} (\theta^{t^{-1}})^M, \lambda^M \right\rangle \\ &= \sum_{t \in [M \backslash G/N]} \left\langle (\theta^{t^{-1}})^M, \lambda^M \right\rangle,\end{aligned}$$

which results in the existence of some element $g \in G$ such that

$$\left\langle (\theta^g)^M, \lambda^M \right\rangle = \left\langle \theta^g, (\lambda^M)_N \right\rangle > 0,$$

as Frobenius Reciprocity again. It means that θ^g is a constituent of $(\lambda^M)_N$. Furthermore, it turns out that $\theta^g = (\lambda^M)_N$, where the right-hand side one will be shown to be monomial. Indeed, it is enough to show that $\theta^g(1) = (\lambda^M)_N(1) = \lambda^M(1)$. According to Problem 6.3a with M/N being solvable (relying on [Isa94, Corollary 5.13]), we have

$$\frac{(\lambda^M)_N(1)}{\theta^g(1)} \mid [M : N] \mid [G : N].$$

On the other hand, from the definition,

$$\begin{aligned}\frac{\lambda^M(1)}{\theta^g(1)} &= \frac{|M|}{|H|} \frac{\lambda(1)}{\theta^g(1)} \\ &= \frac{|N||H|}{|N \cap H||H|} \frac{\lambda(1)}{\theta^g(1)} \\ &= \frac{|N|}{|N \cap H| \theta^{t^{-1}}(1)}\end{aligned}$$

divides $|N|$. As a result, we have

$$\frac{\lambda^M(1)}{\theta^g(1)} \mid (|N|, [G : N]) = 1,$$

which yields $\lambda^M(1) = \theta^g(1)$ as desired. Besides, the following holds as a particular situation of Mackey's Formula (or [Isa94, Exercise 5.2]):

$$(\lambda^M)_N = (\lambda^{HN})_N = (\lambda_{H \cap N})^N,$$

so it is a monomial character of N. To conclude, we have

$$\begin{aligned}\theta &= (\theta^g)^{g^{-1}} \\ &= ((\lambda_{H \cap N})^N)^{g^{-1}} \\ &= ((\lambda_{H \cap N})^{g^{-1}})^{N^{g^{-1}}} \\ &= ((\lambda^{g^{-1}})_{H^{g^{-1}} \cap N})^N\end{aligned}$$

is a monomial character of N. The proof is complete. $\square$

6.5. Let $N \triangleleft G$ with G/N cyclic. Let $\theta \in \mathrm{Irr}(N)$ be invariant in G and suppose that

$$(\theta(1), [G : N]) = 1.$$

Show that θ is extendible to G.

Solution. Recall the fact that θ is invariant in G, i.e. $I_G(\theta) = G$, is equivalent to $\theta^g = \theta$ for all $g \in G$. First, we claim that $\ker(\det\theta) \trianglelefteq G$. Indeed, we denote by $\mathfrak{X}$ the representation of N affording θ. For every element $g \in G$, the representations $\mathfrak{X}$ and $\mathfrak{X}^g$ both afford the same character $\theta = \theta^g$. By [Isa94, Corollary 2.9], $\mathfrak{X}$ and $\mathfrak{X}^g$ are similar, which implies that $\det(\mathfrak{X}(n)) = \det(\mathfrak{X}^g(n))$, for all $g \in G$ and $n \in N$. Therefore, we obtain that

$$\begin{aligned}(\det\theta)(gng^{-1}) &= \det(\mathfrak{X}(gng^{-1}))\\ &= \det(\mathfrak{X}^g(n))\\ &= \det(\mathfrak{X}(n))\\ &= (\det\theta)(n),\end{aligned}$$

for all $g \in G$ and $n \in N$. As a result, if $n \in \ker(\det\theta)$, then $gng^{-1} \in \ker(\det\theta)$ for all $g \in G$, it means that $\ker(\det\theta) \trianglelefteq G$.

Next, we will show that $G/\ker(\det\theta)$ is abelian. In fact, since $|\det\theta(n)| = 1 = \det\theta(1)$ for every $n \in N$, we deduce that $N = Z(\det\theta)$. By [Isa94, Lemma 2.27-(d)], $N/\ker(\det\theta)$ is cyclic. Let $N\tau$ and $\ker(\det\theta)\eta$, respectively, be generators of the cyclic groups G/N and $N/\ker(\det\theta)$, respectively. As a result, every element of $G/\ker(\det\theta)$ is of the form $\ker(\det\theta)\eta^i\tau^j$ where $i, j \in \mathbb{Z}$. With the aim of proving $G/\ker(\det\theta)$ is abelian, it is necessary and sufficient to indicate that $\tau\eta\tau^{-1}\eta^{-1} \in \ker(\det\theta)$. This occurs since

$$\det\theta(\tau\eta\tau^{-1}\eta^{-1}) = \det\theta(\tau\eta\tau^{-1})\det\theta(\eta^{-1}) = \det\theta^\tau(\eta)\det\theta(\eta^{-1}) = \det\theta(\eta)\det\theta(\eta^{-1}) = 1.$$

By [Isa94, Theorem 6.25], it is equivalent to show that $\det\theta$ is extendible to G. Certainly, [Isa94, Lemma 2.22] gives us the existence of a linear character $\widehat{\det\theta}$ of $N/\ker(\det\theta)$ defined as $\det\theta(n) = \widehat{\det\theta}(\ker(\det\theta)n)$. The fact that $G/\ker(\det\theta)$ is abelian enables us to use [Isa94, Lemma 5.5], which deduces that $\widehat{\det\theta}$ is extendible to $G/\ker(\det\theta)$, that is, there is a character, say $\widehat{\chi}$, of $G/\ker(\det\theta)$ such that $\widehat{\chi}_{N/\ker(\det\theta)} = \widehat{\det\theta}$. Using again [Isa94, Lemma 2.22], we obtain a character χ of G defined as $\chi(g) = \widehat{\chi}(\ker(\det\theta)g)$. To conclude, we show that χ is an extension of $\det\theta$. In fact, we have

$$\begin{aligned}\chi_N(n) &= \chi(n)\\ &= \hat{\chi}(\ker(\det\theta)n)\\ &= \hat{\chi}_{N/\ker(\det\theta)}(\ker(\det\theta)n)\\ &= \hat{\det}\,\theta(\ker(\det\theta)n)\\ &= \det\theta(n),\end{aligned}$$

for all $n \in N$. The proof is complete. $\square$

6.6. Let $1 = H_0 \lhd H_1 \lhd \cdots \lhd H_n = G$. Suppose H_i/H_{i-1} is nonabelian for all i. Show that G has an irreducible character χ of degree at least 2^n.

Solution. Let $P(k)$ be the statement that G has an irreducible character of degree at least 2^k, provided that G possesses a subnormal series $1 = H_0 \lhd H_1 \lhd \cdots \lhd H_k = G$ satisfying H_i/H_{i-1} is non-abelian for all indices i. For $k = 1$, as $H_1/H_0 \simeq G$ is non-abelian, it has a non-linear, i.e. of degree greater than or equal to 2, irreducible character. Let an integer $n \in \mathbb{N}$ be given and assume that $P(k)$ holds for all values $1 \leq k \leq n$. Consider a group G having a subnormal series

$$1 = H_0 \lhd H_1 \lhd \cdots \lhd H_{n+1} = G,$$

such that H_i/H_{i-1} is non-abelian for all i. By the induction assumption, H_n has an irreducible character θ of degree at least 2^n. Pick χ as an irreducible constituent of θ^G. Then, we have

$$0 < \langle\theta^G, \chi\rangle = \langle\theta, \chi_{H_n}\rangle,$$

where the equality holds by Frobenius Reciprocity. In other words, θ is an irreducible constituent of χ_{H_n}. According to [Isa94, Lemma 6.8], it follows that $\theta(1) \mid \chi(1)$, which leads to either $\chi(1) = \theta(1)$ or $\chi(1) \geq 2\theta(1)$. When $\chi(1) \geq 2\theta(1)$, then $\chi(1) \geq 2\theta(1) \geq 2^{n+1}$. When $\chi(1) = \theta(1)$, then $\chi_{H_n} = \theta$. Since $H_{n+1}/H_n = G/H_n$ is non-abelian, there exists a non-linear irreducible character β of G/H_n. Using [Isa94, Corollary 6.17], we deduce that $\beta\chi$ is an irreducible character of G having degree $(\beta\chi)(1) = \beta(1)\chi(1) \geq 2\theta(1) \geq 2^{n+1}$. In either cases, it concludes our proof. $\square$

6.7. Let $\mathbb{F}$ be a field of characteristic 5, and let $G = \mathrm{Sym}(\{1, \dots, 5\}) \cong S_5$ act on $V = \langle e_1, \dots, e_5 \rangle_{\mathbb{F}}$ via $\sigma(e_i) = e_{\sigma(i)}$. Consider the submodules $I \subset U \subset V$, where $I = \langle \sum_i e_i \rangle$ and $U = \{\sum_i a_i e_i : \sum_i a_i = 0\}$.

(a) Using the bilinear form $(\sum_i x_i e_i, \sum_i y_i e_i) = \sum_i x_i y_i$, show that $V/I \cong U^*$ as $\mathbb{F}G$-modules.
(b) Show that $\mathrm{Hom}_{\mathbb{F}G}(\mathbb{F}, U) \neq 0$, but $\mathrm{Hom}_{\mathbb{F}G}(U, \mathbb{F}) \cong \mathrm{Hom}_{\mathbb{F}G}(\mathbb{F}, V/I) = 0$.

Solution. (a) It is routine to verify that I and U are $\mathbb{F}G$-modules, where U is of dimension 4 as space over $\mathbb{F}$. Recall that $U^* = \mathrm{Hom}_{\mathbb{F}}(U, \mathbb{F})$ is the dual space of U, whose dimension is of as of U.

Put $u_i = e_i - e_5$ for each $1 \leq i \leq 4$. It is clear that $\{u_i\}_{i=1}^4$ is a basis of U. Denote by $\{u_i^*\}_{i=1}^4$ the dual basis of U^* corresponding to $\{u_i\}_{i=1}^4$, that is,

$$u_i^* \left(\sum_{j=1}^4 x_j u_j \right) = x_i,$$

for all $x_j \in \mathbb{F}$.

Then, we construct a structure of $\mathbb{F}G$-module on U^* by equipping an action of G on U^*. In fact, for each $f \in U^*$ and $\sigma \in G$, we define an operation $\sigma(f) = f \circ \sigma^{-1}$. It is enough to show that $\sigma(\rho(f)) = (\sigma\rho)(f)$, for all $\sigma, \rho \in G$ and $f \in U^*$. Indeed, we have

$$\begin{aligned} \sigma(\rho(f)) &= \sigma(f \circ \rho^{-1}) \\ &= (f \circ \rho^{-1}) \circ \sigma^{-1} \\ &= f \circ (\rho^{-1} \circ \sigma^{-1}) \\ &= f \circ (\sigma\rho)^{-1} \\ &= (\sigma\rho)(f). \end{aligned}$$

Then, we expect to have a so-called element u_5^* which the action of G on U satisfies $\sigma(u_i^*) = u_{\sigma(i)}^*$ for every i. In fact, by letting $u_5^* = -\sum_{i=1}^4 u_i^*$, we will show that $\sigma(u_i^*) = u_{\sigma(i)}^*$ for every $1 \leq i \leq 5$. First, we check that $u_i^* \left(\sum_{i=1}^5 x_i e_i \right) = x_i$ for all $\sum_{i=1}^5 x_i e_i \in U$, i.e. $\sum_{i=1}^5 x_i = 0$. Indeed, we have

$$u_i^* \left(\sum_{i=1}^5 x_i e_i \right) = u_i^* \left(\sum_{i=1}^4 x_i e_i - \sum_{i=1}^4 x_i e_5 \right) = u_i^* \left(\sum_{i=1}^4 x_i u_i \right) = x_i,$$

for every $1 \leq i \leq 4$, and

$$u_5^* \left(\sum_{i=1}^5 x_i e_i \right) = - \left(\sum_{i=1}^4 u_i^* \right) \left(\sum_{i=1}^5 x_i e_i \right) = - \sum_{i=1}^4 x_i = x_5.$$

Then, we obtain that

$$\begin{aligned}\sigma(u_i^*)\left(\sum_{i=1}^5 x_ie_i\right) &= u_i^*\circ\sigma^{-1}\left(\sum_{i=1}^5 x_ie_i\right)\\ &= u_i^*\left(\sum_{i=1}^5 x_ie_{\sigma^{-1}(i)}\right)\\ &= u_i^*\left(\sum_{i=1}^5 x_{\sigma(i)}e_i\right)\\ &= x_{\sigma(i)}\\ &= u_{\sigma(i)}^*\left(\sum_{i=1}^5 x_ie_i\right),\end{aligned}$$

for all $\sum_{i=1}^5 x_ie_i \in U$. Thus, $\sigma(u_i^*) = u_{\sigma(i)}^*$ for every $1\le i\le 5$.

We now construct an $\mathbb{F}G$-isomorphism between V/I and U^*. Consider the map defined as

$$\begin{aligned}\phi : V &\to U^*\\ \sum_{i=1}^5 x_ie_i &\mapsto \sum_{i=1}^5 x_iu_i^*.\end{aligned}$$

It is obvious that ϕ is $\mathbb{F}$-linear from V to U^*. Furthermore, ϕ is an $\mathbb{F}G$-homomorphism since

$$\phi(\sigma(e_i)) = \phi(e_{\sigma(i)}) = u_{\sigma(i)}^* = \sigma(u_i^*) = \sigma(\phi(e_i)).$$

Note that ϕ is clearly surjective by the definition of ϕ. We shall show that $\ker\phi = I$. Firstly, the fact that $\sum_{i=1}^5 u_i^* = 0$ and $\mathrm{char}(\mathbb{F}) = 5$ leads to $I\subseteq\ker\phi$. Secondly, for every $\sum_{i=1}^5 x_ie_i\in\ker\phi$, we have

$$0 = \phi\left(\sum_{i=1}^5 x_ie_i\right) = \sum_{i=1}^5 x_iu_i^*,$$

and hence

$$0 = \left(\sum_{i=1}^5 x_iu_i^*\right)u_j = \left(\sum_{i=1}^4 (x_i-x_5)u_i^*\right)u_j = x_j - x_5$$

for every $1\le j\le 4$. It means that $x_1=\cdots=x_5$, or $\sum_{i=1}^5 x_ie_i\in I$. In conclusion, according to First Isomorphism Theorem, $V/\ker\phi = V/I\cong U^*$ as $\mathbb{F}G$-modules.

(b) Define the map $\theta:\mathbb{F}\to U$ as $\theta(t) = t\sum_{i=1}^4 u_i$. It is straightforward that $\theta\in\mathrm{Hom}_{\mathbb{F}G}(\mathbb{F},U)$ is non-zero (here the action of G on $\mathbb{F}$ is the trivial one). Thus, $\mathrm{Hom}_{\mathbb{F}G}(\mathbb{F},U)\ne 0$.

According to part (a), we establish a natural isomorphism

$$\mathrm{Hom}_{\mathbb{F}G}(U,\mathbb{F})\cong\mathrm{Hom}_{\mathbb{F}G}(\mathbb{F}^*,U^*)\cong\mathrm{Hom}_{\mathbb{F}G}(\mathbb{F},V/I)$$

as $\mathbb{F}$-spaces. For each $f\in\mathrm{Hom}_{\mathbb{F}G}(\mathbb{F},V/I)$, by definition of $\mathbb{F}G$-homomorphism, the map f satisfies that $\sigma(f(1)) = f(\sigma(1)) = f(1)$ for all $\sigma\in G$. Therefore, if we write $f(1) = \sum_{i=1}^5 x_ie_i + I$, we obtain that

$$\sum_{i=1}^5 x_ie_{\sigma(i)} + I = \sigma\left(\sum_{i=1}^5 x_ie_i + I\right) = \sum_{i=1}^5 x_ie_i + I,$$

which yields

$$\sum_{i=1}^{5} \left(x_i - x_{\sigma^{-1}(i)}\right) e_i \in I,$$

for all $\sigma \in G$, or equivalently $x_i - x_{\sigma^{-1}(i)} = x_j - x_{\sigma^{-1}(j)}$ for all $1 \leq i, j \leq 5$. For each pair (i, j), we choose $\sigma = (i\ j)$, and hence we get $x_i - x_j = x_j - x_i$, so $x_i = x_j$. Thus, $f(1) = \overline{1}$. Consequently, $f(x) = xf(1) = xI = I$ for all $f \in \mathrm{Hom}_{\mathbb{F}G}(\mathbb{F}, V/I)$ and $x \in \mathbb{F}$. We conclude that $\mathrm{Hom}_{\mathbb{F}G}(\mathbb{F}, V/I) = 0$. The proof is complete.

$\square$

7.1. Let $N \lhd G$, $H \subseteq G$, with $NH = G$ and $N \cap H = 1$. Show that the following are equivalent:

(a) $C_G(n) \subseteq N$ for all $1 \neq n \in N$;
(b) $C_H(n) = 1$ for all $1 \neq n \in N$;
(c) $C_G(h) \subseteq H$ for all $1 \neq h \in H$;
(d) every $x \in G \setminus N$ is conjugate to an element of H;
(e) if $1 \neq h \in H$, then h is conjugate to every element of Nh.
(f) H is a Frobenius complement in G.

Solution. In fact, G is an (inner) semidirect product of N and H, denoted by $G = N \rtimes H$, which means every element of G can be written uniquely as a product of one element of N and one element of H and further more

$$|N| = \frac{|G|}{|H|}.$$

For convenience, denote by $H = Hg_1, \ldots, Hg_{|N|}$ all of the representatives of $H \backslash G$. Our goal is to establish the following implications: $(a) \Rightarrow (b) \Rightarrow (c) \Rightarrow (e) \Rightarrow (d) \Rightarrow (f) \Rightarrow (a)$.

(a) $\Rightarrow$ (b) For all $1 \neq n \in N$, $C_H(n) \subseteq C_G(n) \cap H \subseteq N \cap H = 1$, so $C_H(n) = 1$.

(b) $\Rightarrow$ (c): For $1 \neq h \in H$, if $g \in C_G(h)$, i.e. $gh = hg$, then $g = nk$ for some $n \in N, k \in H$. Therefore, we have $(nk)h = h(nk)$, so

$$n^{-1}h^{-1}nh = kh^{-1}k^{-1}h \in H.$$

Because $N \lhd G$, then $n^{-1}h^{-1}nh = n^{-1}(h^{-1}nh) \in N$. To sum up, $n^{-1}h^{-1}nh \in H \cap N = 1$, which implies $nh = hn$. The fact that $1 \neq h \in C_H(n)$ leads to $n = 1$ and hence $g \in H$ by the assumption.

(c) $\Rightarrow$ (e): Fix $1 \neq h \in H$. For the purpose of proving statement (e), it is enough to show that $\{nhn^{-1} : n \in N\} = Nh$, or equivalently as $\{nhn^{-1}h^{-1} : n \in N\} = N$. Indeed, since $N \trianglelefteq G$, we have

$$\{n(hn^{-1}h^{-1}) : n \in N\} \subseteq N.$$

In addition, if $n_1hn_1^{-1}h^{-1} = n_2hn_2^{-1}h^{-1}$, for some $n_1, n_2 \in N$, then $n_2^{-1}n_1 \in C_G(h)$. To summarize,

$$n_2^{-1}n_1 \in C_G(h) \cap N \subseteq H \cap N = 1,$$

so $n_1 = n_2$. Hence, $\left|\{nhn^{-1}h^{-1} : n \in N\}\right| = |N|$, which shows that $\{nhn^{-1}h^{-1} : n \in N\} = N$.

(e) $\Rightarrow$ (d): For every $x \in G \setminus N$, we decompose $x = nh \in Nh$ where $n \in N$ and $1 \neq h \in H$. By the assumption, x is conjugate to $h \in H$.

(d) $\Rightarrow$ (f): For every $g \in G \setminus N$, there are some $h \in H$ and $t \in G$ such that $g = h^t$ by the assumption (d). As a result, $g \in H^t$. On the other side, we have $t \in Hg_i$ for some i, so $g \in H^t \subseteq H^{Hg_i} = (H^H)^{g_i} = H^{g_i}$. Therefore, we obtain that

$$G \setminus N \subseteq \bigcup_{i=1}^{|N|} H^{g_i},$$

or equivalently that

$$\begin{aligned}G &= N \cup \bigcup_{i=1}^{|N|} H^{g_i} \\ &= N \cup \bigcup_{i=1}^{|N|} (H \setminus \{1\})^{g_i}.\end{aligned}$$

As a consequence, we get

$$\begin{aligned}|G| &\leq |N| + \left| \bigcup_{i=1}^{|N|} (H \setminus \{1\})^{g_i} \right| \\ &\leq |N| + \sum_{i=1}^{|N|} (|(H \setminus \{1\})^{g_i}|) \\ &= |N| + |N|(|H| - 1) \\ &= |G|.\end{aligned}$$

This occurs if and only if

$$G = N \sqcup \bigsqcup_{i=1}^{|N|} (H \setminus \{1\})^{g_i},$$

which shows that $H \cap H^g = 1$ for every $g \in G \setminus H$.

(f) $\Rightarrow$ (a): Initially, we aim to show that $x^N \cap H \neq \emptyset$ for every $x \in G \setminus N$. In fact, since $N \cap H = 1$ and $N \lhd G$, we deduce that $N \cap H^g = 1$ for every $g \in G$. As a result,

$$N \subseteq \left(G \setminus \bigcup_{i=1}^{|N|} H^{g_i} \right) \cup \{1\}.$$

On the other hand, according to [Isa94, Lemma 7.3], we have

$$\left| \left(G \setminus \bigcup_{i=1}^{|N|} H^{g_i} \right) \cup \{1\} \right| = [G : H] = |N|.$$

Therefore, we obtain that

$$N = \left(G \setminus \bigcup_{i=1}^{|N|} H^{g_i} \right) \cup \{1\},$$

or equivalently that

$$G \setminus N = \bigcup_{i=1}^{|N|} H^{g_i} \setminus \{1\}.$$

It means that, for every $x \in G \setminus N$, there is some index i such that $x \in H^{g_i}$. As a result, we have $x^{g_i^{-1}} \in H$, which leads to $x^G \cap H \neq \emptyset$. Moreover, it follows that

$$\begin{aligned}\emptyset &\neq x^G \cap H \\ &= x^{NH} \cap H \\ &= (x^N \cap H)^H,\end{aligned}$$

which implies that $x^N \cap H \neq \emptyset$. Now, we need to show that $C_G(n) \subseteq N$ for all $1 \neq n \in N$, provided that $x^N \cap H \neq \emptyset$ for all $x \notin N$. Assume by contradiction that there exist an element $n \in N$ and an element $g \notin N$ such that $gn = ng$. The fact that $g^N \cap H \neq \emptyset$ leads to the existence of an element $h \in H$ such that $h = g^z$ for some $z \in N$. We obtain

$$h^{z^{-1}} = g = g^n = (z^{-1}n)^{-1}h(z^{-1}n) = h^{z^{-1}n},$$

so $h = h^{n^z} \in H \cap H^{n^z}$ is a non-trivial as $g \neq 1$, which leads to $H \cap H^{n^z} \neq 1$. Since H is a Frobenius complement of G, we must have $n^z \in H$. Consequently, $n^z = z^{-1}nz \in H \cap N = 1$, it means that $n = 1$, a contradiction! Therefore, $C_G(n) \subseteq N$ for all $1 \neq n \in N$.

$\square$

7.2. Let $H \subseteq G$ with $M \triangleleft H$ and suppose that $H \cap H^x \subseteq M$ whenever $x \notin H$. Show that there exists $N \triangleleft G$ with $NH = G$ and $N \cap H = M$.

Solution. Denote by $H = Hg_1, Hg_2, \ldots, Hg_{[G:H]}$ all of the right cosets $H\backslash G$. Put

$$N = G \setminus \bigcup_{x \in G} (H \setminus M)^x.$$

We will show that N satisfies the conclusion. To begin with, we need the following lemma:

Lemma 14. *With the above assumption, the following statements hold:*

(a) $|N| = \frac{|G||M|}{|H|}$.
(b) *If $W \triangleleft G$ and $W \cap H \subseteq M$, then $W \subseteq N$.*
(c) *If θ is a class function of H satisfying $\theta(m) = 0$ for all $m \in M$, then $(\theta^G)_H = \theta$.*

Proof of the Lemma 14. (a) If $xy^{-1} \in H$, then

$$(H \setminus M)^x = \left((H \setminus M)^{xy^{-1}}\right)^y = \left(H^{xy^{-1}} \setminus M^{xy^{-1}}\right)^y = (H \setminus M)^y,$$

as $M \triangleleft H$. In converse, if $xy^{-1} \notin H$, then

$$\begin{aligned}(H \setminus M)^x \cap (H \setminus M)^y &= \left((H \setminus M)^{xy^{-1}} \cap (H \setminus M)\right)^y \\ &\subseteq \left(H^{xy^{-1}} \cap (H \setminus M)\right)^y \\ &\subseteq \left((H^{xy^{-1}} \cap H) \setminus M\right)^y \\ &= \emptyset.\end{aligned}$$

Thus, we obtain that $N = G \setminus \bigcup_{x \in G}(H \setminus M)^x = G \setminus \bigsqcup_{i=1}^{[G:H]}(H \setminus M)^{g_i}$. As a result,

$$\begin{aligned}|N| &= |G| - \sum_{i=1}^{[G:H]} |(H \setminus M)^{g_i}| \\ &= |G| - [G : H](|H| - |M|) \\ &= \frac{|G||M|}{|H|}.\end{aligned}$$

(b) Next, if $W \triangleleft G$ and $W \cap H \subseteq M$, then $W \cap (H \setminus M) = \emptyset$, and so $W \cap (H \setminus M)^g = \emptyset$ for all $g \in G$. Therefore,

$$W \subseteq G \setminus \bigsqcup_{i=1}^{[G:H]} (H \setminus M)^{g_i} = N.$$

(c) Let θ be a class function of H such that $\theta(m) = 0$ for all $m \in M$. For any $h \in H$ and $g \notin H$, we obtain either $h^g \notin H$ or $h^g \in H^g \cap H \subseteq M$. In either case, we have $\theta^\circ(h^g) = 0$. As a consequence, we have

$$\theta^G(h) = \frac{1}{|H|}\sum_{g\in G}\theta^\circ(h^g) = \frac{1}{|H|}\sum_{g\in H}\theta^\circ(h^g) = \frac{1}{|H|}|H|\theta(h) = \theta(h).$$

□

Return to the main problem. For every $\phi \in \mathrm{Irr}(H)$ such that $M \leq \ker\phi$, the class function

$$\vartheta = \phi - \phi(1)1_H$$

satisfies $\vartheta(m) = 0$ for all $m \in M$ (here for abbreviation, we simplify by writing ϑ instead of ϑ_ϕ). We gain that

$$\langle \vartheta^G, 1_G\rangle = \langle \vartheta, (1_G)_H\rangle = \langle \vartheta, 1_H\rangle = -\phi(1),$$

and, by Frobenius Reciprocity and Lemma 14-(c), that

$$\langle \vartheta^G, \vartheta^G\rangle = \langle \vartheta, (\vartheta^G)_H\rangle = \langle \vartheta, \vartheta\rangle = 1 + \phi(1)^2.$$

Set $\phi^* = \vartheta^G + \phi(1)1_G$. Notice that since ϑ is a difference of characters, so are ϑ^G and, consequently, ϕ^*. We claim that ϕ^* is an irreducible character of G. Indeed, the computation

$$\begin{aligned}\langle \phi^*, \phi^*\rangle &= \langle \vartheta^G + \phi(1)1_G, \vartheta^G + \phi(1)1_G\rangle\\ &= \langle \vartheta^G, \vartheta^G\rangle + 2\phi(1)\langle \vartheta^G, 1_G\rangle + \phi(1)^2\langle 1_G, 1_G\rangle\\ &= 1 + \phi(1)^2 - 2\phi(1)^2 + \phi(1)^2\\ &= 1.\end{aligned}$$

yields that ϕ^* is either a plus or minus of an irreducible character of G. Nonetheless, the latter situation cannot happen since

$$(\phi^*)_H = (\vartheta^G + \phi(1)1_G)_H = (\vartheta^G)_H + \phi(1)1_H = \vartheta + \phi(1)1_H = \phi,$$

In particular, $\phi^*(1) = (\phi^*)_H(1) = \phi(1) > 0$, and thus $\phi^* \in \mathrm{Irr}(G)$. To sum up, for every $\phi \in \mathrm{Irr}(H)$ satisfying $M \leq \ker\phi$, we are able to construct a so-called extension $\phi^* \in \mathrm{Irr}(G)$ of ϕ.

Next, our goal is to show that

$$N = \bigcap_{\phi\in\mathrm{Irr}(H); M\leq\ker\phi} \ker\phi^* \trianglelefteq G.$$

If $n \in N$, which is equivalent to $n \notin \bigcup_{x\in G}(H\backslash M)^x$, then $n^x \notin H\backslash M$ for every $x \in G$. Consequently, either $n^x \notin H$ or $n^x \in M$ for every $x \in G$. In either case, $\vartheta^\circ(n^x) = 0$, so we derive that

$$\phi^*(n) - \phi(1) = \vartheta^G(n) = \frac{1}{|H|}\sum_{x\in G}\vartheta^\circ(n^x) = 0.$$

It means that $n \in \ker\phi^*$, for all $\phi \in \mathrm{Irr}(H)$ satifying $M \leq \ker\phi$, or equivalently that

$$n \in \bigcap_{\phi\in\mathrm{Irr}(H); M\leq\ker\phi} \ker\phi^*.$$

Conversely, by Lemma 14-(b), it is enough to indicate that $\bigcap_{\phi\in\mathrm{Irr}(H); M\leq\ker\phi}\ker\phi^* \cap H \subseteq M$. However, as above, it is clear that for any $x \in \bigcap_\phi \ker\phi^* \cap H$, we have

$$\phi(x) = (\phi^*)_H(x) = \phi^*(x) = \phi^*(1) = \phi(1),$$

for every $\phi \in \mathrm{Irr}(H)$ such that $M \leq \ker\phi$. It implies that

$$x \in \bigcap_{\phi\in\mathrm{Irr}(H); M\leq\ker\phi} \ker\phi = M.$$

Thus, $N = \bigcap_\phi \ker \phi^* \lhd G$.

Finally, we have that

$$\begin{aligned} N \cap H &= \left(\bigcap_{\phi \in \mathrm{Irr}(H); M \leq \ker \phi} \ker \phi^* \right) \cap H \\ &= \bigcap_{\phi \in \mathrm{Irr}(H); M \leq \ker \phi} (\ker \phi^* \cap H) \\ &= \bigcap_{\phi \in \mathrm{Irr}(H); M \leq \ker \phi} \ker (\phi^*)_H \\ &= \bigcap_{\phi \in \mathrm{Irr}(H); M \leq \ker \phi} \ker \phi \\ &= M. \end{aligned}$$

Consequently, it follows that $|NH| = \frac{|N||H|}{|N \cap H|} = \frac{|N||H|}{|M|} = |G|$ (cf. Lemma 14) and hence $NH = G$. The proof is complete. $\square$

7.3. Let $H \subseteq G$ and $\xi \in \mathrm{Irr}(H)$. Suppose $(\xi - \xi(1)1_H)^G = \vartheta$ and $\langle \vartheta, \vartheta \rangle = 1 + \xi(1)^2$. Show that there exists $N \lhd G$ with $N \cap H = \ker \xi$ and every $x \in G \setminus N$ conjugate to some element of H.

Solution. Notice that $\vartheta \neq 0$, which leads to $\xi \neq 1_H$. By Frobenius Reciprocity,

$$\langle \vartheta, 1_G \rangle = \langle (\xi - \xi(1)1_H)^G, 1_G \rangle = \langle \xi - \xi(1)1_H, (1_G)_H \rangle = \langle \xi - \xi(1)1_H, 1_H \rangle = -\xi(1).$$

Then, by setting $\xi^* = \vartheta + \xi(1)1_G$, we have

$$\begin{aligned} \langle \xi^*, \xi^* \rangle &= \langle \vartheta + \xi(1)1_G, \vartheta + \xi(1)1_G \rangle \\ &= \langle \vartheta, \vartheta \rangle + 2\xi(1)\langle \vartheta, 1_G \rangle + \xi(1)^2 \langle 1_G, 1_G \rangle \\ &= 1 + \xi(1)^2 - 2\xi(1)^2 + \xi(1)^2 \\ &= 1. \end{aligned}$$

As the argument in Problem 7.2, because $\xi - \xi(1)1_G$ is a difference of characters, so are $(\xi - \xi(1)1_G)^G = \vartheta$ and ξ^*. Therefore, ξ^* is either a plus or minus of an irreducible character. In addition,

$$\xi^*(1) = \vartheta(1) + \xi(1) = [G : H](\xi(1) - \xi(1)) + \xi(1) = \xi(1) > 0,$$

so $\xi^* \in \mathrm{Irr}(G)$. Using Frobenius Reciprocity again, we obtain that

$$\begin{aligned} 1 + \xi(1)^2 &= \langle \vartheta, \vartheta \rangle \\ &= \left\langle (\xi - \xi(1)1_H)^G, \xi^* - \xi(1)1_G \right\rangle \\ &= \langle \xi - \xi(1)1_H, (\xi^* - \xi(1)1_G)_H \rangle \\ &= \langle \xi - \xi(1)1_H, (\xi^*)_H - \xi(1)1_H \rangle \\ &= \langle \xi, (\xi^*)_H \rangle + \xi(1)^2 - \xi(1)\langle 1_H, (\xi^*)_H \rangle, \end{aligned}$$

which is reformulated as

$$\langle \xi, (\xi^*)_H \rangle = 1 + \xi(1)\langle 1_H, (\xi^*)_H \rangle \geq 1.$$

Thus, ξ is an irreducible constituent of $(\xi^*)_H$. Furthermore, the fact that $\xi(1) = \xi^*(1)$ leads to $(\xi^*)_H = \xi$.

Set $N = \ker \xi^* \lhd G$. We have

$$N \cap H = \ker \xi^* \cap H = \ker(\xi^*)_H = \ker \xi.$$

Moreover, for every $x \in G \setminus N$, we have

$$\begin{aligned}0 &\neq \xi^*(x) - \xi(1)\\ &= \vartheta(x)\\ &= \left(\xi - \xi(1)1_H\right)^G(x)\\ &= \frac{1}{|H|}\sum_{g\in G}\left(\xi - \xi(1)1_H\right)^\circ(x^g).\end{aligned}$$

Consequently, there is $g \in G$ such that $\left(\xi - \xi(1)1_H\right)^\circ(x^g) \neq 0$. This occurs if and only if $x^g \in H$. The proof is complete. $\square$

7.4. Let $H < G$ and suppose induction to G is an isometry on $\mathbb{Z}[\mathrm{Irr}(H)]^\circ$. Show that H is a Frobenius complement in G.

Solution. Denote by $H = Hg_1, H_{g_2}, \ldots, H_{g_n}$ all of the right cosets $H\backslash G$. The assumption can be rephrased as $\langle \chi^G, \xi^G\rangle = \langle \chi, \xi\rangle$ for all $\chi, \xi \in \mathbb{Z}[\mathrm{Irr}(H)]$ satisfying $\chi(1) = \xi(1) = 0$. For each $\phi \in \mathrm{Irr}(H)$, we set $\vartheta = \phi - \phi(1)1_H$, so $\vartheta(1) = 0$. Note that $\langle \vartheta^G, 1_G\rangle = \langle \vartheta, 1_H\rangle = -\phi(1)$ by Frobenius Reciprocity. Moreover, as the rephrased assumption, we obtain that

$$\langle \vartheta^G, \vartheta^G\rangle = \langle \vartheta, \vartheta\rangle = 1 + \phi(1)^2,$$

As a result, by putting $\phi^* = \vartheta^G + \phi(1)1_G$, it follows that

$$\begin{aligned}\langle \phi^*, \phi^*\rangle &= \langle \vartheta^G, \vartheta^G\rangle + \langle \vartheta^G, \phi(1)1_G\rangle + \langle \phi(1)1_G, \vartheta^G\rangle + \langle \phi(1)1_G, \phi(1)1_G\rangle\\ &= 1 + \phi(1)^2 - \phi(1)^2 - \phi(1)^2 + \phi(1)^2\\ &= 1.\end{aligned}$$

On the other hand, because $\vartheta \in \mathbb{Z}[\mathrm{Irr}(H)]$, then $\vartheta^G \in \mathbb{Z}[\mathrm{Irr}(G)]$, implying that $\phi^* \in \mathbb{Z}[\mathrm{Irr}(G)]$ as well. The fact that $\langle \phi^*, \phi^*\rangle = 1$ leads to that either ϕ^* or $-\phi^*$ is an irreducible character G. In addition,

$$\phi^*(1) = \vartheta^G(1) + \phi(1) = [G:H]\vartheta(1) + \phi(1) = \phi(1) > 0,$$

so $\phi^* \in \mathrm{Irr}(G)$. Using Frobenius Reciprocity, we have

$$\begin{aligned}1 + \phi(1)^2 &= \langle \vartheta^G, \vartheta^G\rangle\\ &= \left\langle (\phi - \phi(1)1_H)^G, \phi^* - \phi(1)1_G\right\rangle\\ &= \langle \phi - \phi(1)1_H, (\phi^*)_H - \phi(1)1_H\rangle\\ &= \langle \phi, (\phi^*)_H\rangle + \phi(1)^2 - \phi(1)\langle \phi, 1_H\rangle - \phi(1)\langle 1_H, (\phi^*)_H\rangle,\end{aligned}$$

so

$$\langle \phi, (\phi^*)_H\rangle = 1 + \phi(1)\langle 1_H, \phi + (\phi^*)_H\rangle \geq 1.$$

Thus, ϕ is an irreducible constituent of $(\phi^*)_H$. Furthermore, $(\phi^*)_H = \phi$ for $\phi^*(1) = \phi(1)$. To summarize, every irreducible character ϕ of H corresponds to an irreducible character ϕ^* of G such that $(\phi^*)_H = \phi$.

Set

$$M = \bigcap_{\phi\in\mathrm{Irr}(H)} \ker\phi^* \trianglelefteq G,$$

and

$$N = \left(G \setminus \bigcup_{g\in G} H^x\right) \cup \{1\} = G \setminus \bigcup_{i=1}^{[G:H]} (H \setminus \{1\})^{g_i}.$$

We will show that $M = N$. Indeed,

$$M \cap H = \bigcap_{\phi \in \mathrm{Irr}(H)} (\ker \phi^* \cap H) = \bigcap_{\phi \in \mathrm{Irr}(H)} \ker(\phi^*)_H = \bigcap_{\phi \in \mathrm{Irr}(H)} \ker \phi = 1,$$

cf. [Isa94, Lemma 2.21]. As a result, $M \cap H^x = 1$ for all $x \in G$, as $M \trianglelefteq G$, which implies

$$M \subseteq \left(G \setminus \bigcup_{g \in G} H^x \right) \cup \{1\} = N.$$

Conversely, if $x \in N \setminus \{1\}$, it means that x is not conjugate to any elements of H, then

$$\phi^*(x) - \phi^*(1) = \phi^*(x) - \phi(1) = \vartheta^G(x) = \frac{1}{|H|} \sum_{g \in G} \vartheta^\circ(x^g) = 0,$$

or equivalently $x \in \ker \phi^*$. Note that the statement we just have shown holds for every irreducible character ϕ of H. Therefore, we get $x \in \bigcap_{\phi \in \mathrm{Irr}(H)} \ker \phi^* = M$. Thus $M = N$. We further gain the following inequality

$$\begin{aligned}
|M| &= |N| \\
&= \left| G \setminus \bigcup_{i=1}^{[G:H]} (H \setminus \{1\})^{g_i} \right| \\
&= |G| - \left| \bigcup_{i=1}^{[G:H]} (H \setminus \{1\})^{g_i} \right| \\
&\geq |G| - \sum_{i=1}^{[G:H]} |(H \setminus \{1\})^{g_i}| \\
&= |G| - [G : H](|H| - 1) \\
&= [G : H].
\end{aligned}$$

Therefore,

$$|G| \geq |MH| = \frac{|M||H|}{|M \cap H|} = |M||H| \geq [G : H]|H| = |G|.$$

This occurs if and only if $H \cap H^g = 1$ for all $g \notin H$, or equivalently, H is a Frobenius complement of G. The proof is complete. □

7.5. Let A be any nontrivial subgroup of the multiplicative group of the finite field $\mathbb{F}_q$, and consider the group G of all maps $\phi : x \mapsto ax + b$ on $\mathbb{F}_q$, where $a \in A$ and $b \in \mathbb{F}_q$, under the usual composition. Show that G is a Frobenius group.

Solution. It is routine to check that the identity of G is the identity map $\mathrm{id}_{\mathbb{F}_q}$ and the inverse element of $\phi : x \mapsto ax + b$ is $\phi^{-1} : x \mapsto a^{-1}x - a^{-1}b$. We claim that the set H consisting of all maps $\alpha_a : x \mapsto ax$, where $a \in A$, is a Frobenius complement in G. Indeed, we see that H is a nontrivial proper subgroup of G. It remains to show that $H \cap H^\beta = 1$ for every $\beta \notin H$. In fact, for every non-trivial element α_a, i.e. $a \neq 1$, of H and $\beta : x \mapsto \tau x + \eta$ of $G \setminus H$, it follows that

$$\begin{aligned}\alpha_a^\beta(x) &= \beta^{-1}\alpha_a\beta(x)\\ &= \beta^{-1}\alpha_a(\tau x + \eta)\\ &= \beta^{-1}(a\tau x + a\eta)\\ &= \tau^{-1}(a\tau x + a\eta) - \tau^{-1}\eta\\ &= ax + \tau^{-1}\eta(a-1),\end{aligned}$$

for every element x. It means that α_a^β is not an element of H since $a \neq 1$ and $\eta \neq 0$. The proof is complete. ☐

7.6. Let V be a 2-dimensional vector space over the field $\mathbb{F}_q$ of $q \geq 4$ elements. Consider the group $G = \mathrm{SL}(V)$ of all linear transformations of V with determinant 1 and its action on the set Ω of 1-dimensional subspaces of V. Show that the induced action of $G/Z(G)$ on Ω yields a Zassenhaus group.

Proof. It is clear that $|\Omega| = q+1$ and $Z(G) = \{\pm \mathrm{I}_2\}$, and so the action of $Z(G)$ on a finite set Ω is trivial. As a result, the induced action of $G/Z(G)$ on Ω is well-defined.

First, we show that $G/Z(G)$ acts doubly-transitively on Ω. It is equivalent to show that for any $U_1, U_2, W_1, W_2 \in \Omega$ such that $U_1 \neq U_2$ and $W_1 \neq W_2$, there exists an element $\overline{g} \in G/Z(G)$ satisfying $g(U_i) = W_i$ where $i = 1, 2$. Let u_1, u_2, w_1, w_2, respectively, generates U_1, U_2, W_1, W_2, respectively. Since $U_1 \neq U_2$ and $W_1 \neq W_2$, we see that $\{u_1, u_2\}$ and $\{w_1, w_2\}$ are two $\mathbb{F}_q$-bases of V. Let A be the transition matrix of the basis $\{w_1, w_2\}$ to $\{u_1, u_2\}$. Consider a linear transformation g defined as $g(u_1) = \frac{1}{\det A} w_1$ and $g(u_2) = w_2$. In fact, it is simple to verify that $g \in G$ and $\overline{g}(U_i) = W_i$ where $i = 1, 2$.

Next, we prove that only the identity element of $G/Z(G)$ fixes more than two elements of Ω. Let V_1, V_2, V_3, respectively, be elements of Ω generated by v_1, v_2, v_3, respectively, such that $V_i \neq V_j$ for all $i \neq j$ and assume that $\overline{g}$ is an element of $G/Z(G)$ satisfying $\overline{g}(V_i) = V_i$ for every $1 \leq i \leq 3$. Equivalently, we have $g(v_i) = a_i v_i \in V_i$ for some $a_i \neq 0$, $1 \leq i \leq 3$. Note that $\{v_1, v_2\}$ is a basis of V as $V_1 \neq V_2$. Then, we write $v_3 = xv_1 + yv_2$ with $x, y \neq 0$ since $v_3 \notin V_i$ for $i = 1, 2$. The equality $\overline{g}(v_3) = a_3 v_3$ is equivalent to $xa_1v_1 + ya_2v_2 = a_3xv_1 + a_3yv_2$, so $(a_1 - a_3)xv_1 = (a_3 - a_2)yv_2$. Because $\{v_1, v_2\}$ is a basis of V and $x, y \neq 0$, we obtain that $a_1 = a_3 = a_2$. Therefore, the matrix form of g corresponding to basis $\{v_1, v_2\}$ is $a_1\mathrm{I}_2$. Since $\det(g) = 1$, we get that $a_1^2 = 1$, or equivalently, $a_1 = \pm 1$. Hence $\overline{g} = \overline{\mathrm{I}_2}$.

Finally, for all $T_1, T_2 \in \Omega$, we prove that

$$\mathrm{Stab}_{\{T_1\}\{T_2\}}(G/Z(G)) = \{\overline{g} \in G/Z(G) : \overline{g}(T_1) = T_1, \overline{g}(T_2) = T_2\}$$

is a nontrivial subgroup of $G/Z(G)$. If $T_1 = T_2$, then $\mathrm{Stab}_{\{T_1\}\{T_2\}}(G/Z(G)) = \mathrm{Stab}_{\{T_2\}}(G/Z(G))$. Because $|\Omega| = q + 1 > 3$, there are two other distinct elements $T_3, T_4 \in \Omega$. Since $G/Z(G)$ acts doubly-transitively on Ω, there is an element $\overline{g} \in G$ such that $\overline{g}(T_2) = T_2$ and $\overline{g}(T_3) = T_4$. It is routine to check that $\overline{g} \in \mathrm{Stab}_{\{T_2\}}(G/Z(G)) \setminus (Z(G)/Z(G))$, so $\mathrm{Stab}_{\{T_2\}}(G/Z(G))$ is non-trivial. Otherwise, let t_i be a vector generating T_i for $i = 1, 2$. Since $T_1 \neq T_2$, $\{t_1, t_2\}$ is a basis of V. Consider g_a is a linear transformation satisfying $g_a(t_1) = at_1$ and $g_a(t_2) = a^{-1}t_2$ for each $a \in \mathbb{F}_q \setminus \{0\}$. The matrix form of g_a corresponding to basis $\{g_1, g_2\}$ is $\mathrm{diag}(a, a^{-1})$ of determinant 1, so $g_a \in G$. It is clear to check that $\overline{g_a} \in \mathrm{Stab}_{\{T_1\}\{T_2\}}(G/Z(G))$ and $\overline{g_a} \neq \overline{\mathrm{I}_2}$ for each $a \in \mathbb{F}_q \setminus \{0, \pm 1\}$. To sum up, $\mathrm{Stab}_{\{T_1\}\{T_2\}}(G/Z(G))$ is a nontrivial subgroup of $G/Z(G)$. The proof is complete. ☐

References

[Isa94] I.M. Isaacs. *Character Theory of Finite Groups*. Dover books on advanced mathematics. Dover, 1994. ISBN: 9780486680149. URL: https://books.google.com.vn/books?id=MeE7BFXwQroC.

[Rot02] J.J. Rotman. *Advanced Modern Algebra*. Recording for the Blind & Dyslexic, 2002. ISBN: 9780821884201. URL: https://books.google.com.vn/books?id=RGzK%5C_DOTijsC.

[1] Faculty of Mathematics and Computer Science, University of Science, Ho Chi Minh City, Vietnam;

[2] Vietnam National University, Ho Chi Minh City, Vietnam