Part 1: Groups and Character Theory

Question 1. Let $G$ be a group of order 21.

a. Determine all possible values of $n$, where $n$ is the number of conjugacy classes of $G$. (I.e., for each positive integer $n$, determine whether or not there is a group of order 21 having exactly $n$ conjugacy classes.)

Claim: The only possible values for $n$ are 5, 21.

Proof. Let $G$ be a group of order 21. By Sylow’s Theorems, the Sylow 7-subgroup of $G$, $P_7$, is normal in $G$. Let $P_3$ be a Sylow 3-subgroup of $G$. Then $P_7 \cap P_3 = \langle e_G \rangle$, $G = P_7 P_3$, and thus $G = P_7 \rtimes_p P_3$ for some $\varphi : P_3 \to \text{Aut}(P_7) \cong (\mathbb{Z}/7\mathbb{Z})^* \cong \mathbb{Z}/6\mathbb{Z}$.

Suppose $P_3 = \langle a \rangle$ and $P_7 = \langle b \rangle$. By a theorem, the elements of $\text{Aut}(P_7)$ are of the form $\psi_b$, where $\psi_b(x) = x^b$. Then there are three possibilities for $\varphi(a)$: $\psi_1$, $\psi_2$, or $\psi_4$. If $\varphi(a) = \psi_1$, then the map is trivial, and we get the usual direct product, so $G = \mathbb{Z}/21\mathbb{Z}$. In this case, as $G$ is abelian, there are $|G| = 21$ distinct conjugacy classes.

Let $\tau \in \text{Aut}(P_3)$ be the inversion map, i.e., $\tau(x) = a^{-1} = a^2$. Suppose $\varphi(a) = \psi_2$. Then $\varphi_\tau(a) = \psi_4$, the other nontrivial map automorphism of $P_7$ having order 2. It is then straightforward to check that $P_7 \rtimes_{\psi} P_3 \cong P_7 \rtimes_{\psi_\tau} P_3$ via the map $(x,y) \mapsto (x,\tau^{-1}(y))$. Therefore, there is only one nonabelian group of order 21. For the computations that follow, we use $P_7 \rtimes_{\psi} P_3$.

In this case, $ab = (1, a) (b^2, a) = (b^2, a^2)$, so we claim that $G = \langle a, b^3 = b^7 = e_G, ab = b^2a \rangle$. It is clear that $\langle a, b^3 = b^7 = e_G, ab = b^2a \rangle \leq G$, but using the relations given, we can rewrite any word in $\langle a, b^3 = b^7 = e_G, ab = b^2a \rangle$ as $b^n a^m$, where $0 \leq m \leq 6$ and $0 \leq n \leq 2$. As there are seven choices for $m$ and three for $n$, there are exactly 21 elements of $\langle a, b^3 = b^7 = e_G, ab = b^2a \rangle$. Thus, $G = \langle a, b^3 = b^7 = e_G, ab = b^2a \rangle$. One may perform computations to find 5 conjugacy classes (realizing that $P_7 < G$, so any conjugacy class containing an element which is a power of $b$ will be contained in $P_7$): $\langle e_G \rangle$, $\{ b, b^2, b^4 \}$, $\{ b^5, b^6, b^8 \}$, $\{ a, b^6a, b^5a, b^3a, b^3, b^5, b^2a, ba \}$, and $\{ a^2, b^6a^2, b^5a^2, b^3a^2, b^2a^2, ba^2 \}$. \[\square\]

b. Determine the possible decompositions of the group $C[G]$ as a product of matrix rings. (I.e., find all possible products $\prod_{i=1}^r M_{n_i} (D_i)$ which are isomorphic as rings to $C[G]$ for some group $G$ of order 21, where $C$ is the field of complex numbers, each $D_i$ is a division ring, and $M_{n_i} (D_i)$ is the ring of $n_i \times n_i$ matrices with entries in $D_i$.)

Claim: The two possibilities are $C[G] \cong \bigoplus_{i=1}^{21} C$ and $C[G] \cong C \oplus C \oplus C \oplus M_3(C) \oplus M_2(C)$ following from $n = 21, 5$, respectively.

Proof. In either case, since $C$ is algebraically closed, we have that $D_i = C$ for all $i$. In the case of 21 conjugacy classes, $G$ is abelian, and via a proof similar to part of the proof Question 7 on this exam, each matrix ring in the decomposition afforded by Wedderburn’s Theorem is a ring of $1 \times 1$ matrices, i.e., $C$ itself. This gives the first decomposition.

In the second case (5 conjugacy classes), we have $\sum_{i=1}^5 n_i^2 = 21$, where $n_i | 21$ for each $i$. Thus, the possibilities for $n_i$ are 1, 3, 7, 21. But notice that no $n_i$ is 7 or 21, as $7^2, 21^2 > 21$. We may assume that $n_1 = 1$ (to account for the trivial character), so $n_2^2 + n_3^2 + n_4^2 + n_5^2 = 20$. But, to sum to 20, at least 2 of the $n_i$’s must be 3, and yet we must have exactly 2 $n_i$’s equal to 3, else the sum will exceed 20. Thus we may take $n_2 = n_3 = 1$ and $n_4 = n_5 = 3$, proving the claim. \[\square\]

Question 2. For this problem you may assume that any finite group having a solvable quotient by a solvable normal subgroup is solvable. You may assume Sylow’s Theorems. You may assume that if the order of a finite group $G$ is the product of at most three (possibly non-distinct) primes, then $G$ is solvable. You may assume that the commutator subgroup of a group is normal. You may also assume that $A_n$ is simple for $n > 4$. Prove everything else that you use or claim in your arguments.

a. If $p$ is prime and $i \geq 0$ is an integer, prove that a group $G$ of order $p^i$ is solvable.

Proof. We proceed by induction on $i$. If $i = 0$, then $|G| = 1$, and thus is trivially solvable. Suppose now for a positive integer $k$ we have that a group is solvable whenever its order is $p^i$ for $i < k$. By the class equation, we may write $p^k = |G| = |Z(G)| + \sum_{i=1}^r |G : C_G(s_i)|$, where the $s_i$’s are representatives of distinct conjugacy classes. As $p$ divides $|G|$, and $s_i \notin Z(G)$ for all $i$ (thus implying that $|G : C_G(s_i)| > 1$ for each $i$), we find that $p$ divides $|Z(G)|$. Thus, since $Z(G)$
is abelian, it is solvable (as it trivially has a solvable series), and since $|Z(G)| > 1$, we find that $|G/Z(G)| = p^j$ for some $j < k$, so consequently $G/Z(G)$ is solvable by induction. Finally, as we have shown that $G$ has a solvable quotient by a solvable normal subgroup (in our case, $Z(G)$), we conclude that $G$ is solvable. ■

b. Find the least positive integer $n$ such that there is a non-solvable group of order $n$. Justify your answer; in particular, justify that all groups of order less than $n$ are solvable.

Claim: The least positive $n$ such that there is a non-solvable group of order $n$ is $n = 60$.

Proof. We first note that there is a non-solvable group of order 60, namely $A_5$, which we may assume is simple. As it is simple, it has no nontrivial normal subgroups, hence its only normal series is $(e_{A_5}) < A_5$. As $A_5$ is nonabelian, $A_5/e_{A_5} = A_5$ is nonabelian, whence $A_5$ has no solvable series. Since a group is solvable if and only if it has a solvable series, we find that $A_5$ is not solvable. It remains to be seen that every group $G$ having order less than 60 is solvable, which we now show. Consider the table:

<table>
<thead>
<tr>
<th>Order</th>
<th>Prime Factorization</th>
<th>Why Solvable?</th>
<th>Order</th>
<th>Prime Factorization</th>
<th>Why Solvable?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>NA</td>
<td>Trivially</td>
<td>31</td>
<td>31</td>
<td>Part a.</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>Part a.</td>
<td>32</td>
<td>2^5</td>
<td>Part a.</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>Part a.</td>
<td>33</td>
<td>3 · 11</td>
<td>Product of ≤ 3 primes</td>
</tr>
<tr>
<td>4</td>
<td>2^2</td>
<td>Part a.</td>
<td>34</td>
<td>2 · 17</td>
<td>Product of ≤ 3 primes</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>Part a.</td>
<td>35</td>
<td>5 · 7</td>
<td>Product of ≤ 3 primes</td>
</tr>
<tr>
<td>6</td>
<td>2 · 3</td>
<td>Product of ≤ 3 primes</td>
<td>36</td>
<td>2^2 · 3^2</td>
<td>See below</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>Part a.</td>
<td>37</td>
<td>7</td>
<td>Part a.</td>
</tr>
<tr>
<td>8</td>
<td>2^3</td>
<td>Part a.</td>
<td>38</td>
<td>2 · 18</td>
<td>Product of ≤ 3 primes</td>
</tr>
<tr>
<td>9</td>
<td>3^2</td>
<td>Part a.</td>
<td>39</td>
<td>3 · 13</td>
<td>Product of ≤ 3 primes</td>
</tr>
<tr>
<td>10</td>
<td>2 · 5</td>
<td>Product of ≤ 3 primes</td>
<td>40</td>
<td>2^3 · 5</td>
<td>See below</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>Part a.</td>
<td>41</td>
<td>2 · 11</td>
<td>Product of ≤ 3 primes</td>
</tr>
<tr>
<td>12</td>
<td>2^2 · 3</td>
<td>Product of ≤ 3 primes</td>
<td>42</td>
<td>2 · 3 · 7</td>
<td>Part a.</td>
</tr>
<tr>
<td>13</td>
<td>13</td>
<td>Part a.</td>
<td>43</td>
<td>13</td>
<td>Part a.</td>
</tr>
<tr>
<td>14</td>
<td>2 · 7</td>
<td>Product of ≤ 3 primes</td>
<td>44</td>
<td>2^2 · 11</td>
<td>Product of ≤ 3 primes</td>
</tr>
<tr>
<td>15</td>
<td>3 · 5</td>
<td>Product of ≤ 3 primes</td>
<td>45</td>
<td>3^2 · 5</td>
<td>Product of ≤ 3 primes</td>
</tr>
<tr>
<td>16</td>
<td>2^4</td>
<td>Part a.</td>
<td>46</td>
<td>2 · 23</td>
<td>Part a.</td>
</tr>
<tr>
<td>17</td>
<td>17</td>
<td>Part a.</td>
<td>47</td>
<td>11</td>
<td>See below</td>
</tr>
<tr>
<td>18</td>
<td>2 · 3^2</td>
<td>Product of ≤ 3 primes</td>
<td>48</td>
<td>2^4 · 3</td>
<td>Part a.</td>
</tr>
<tr>
<td>19</td>
<td>19</td>
<td>Part a.</td>
<td>49</td>
<td>7^2</td>
<td>Part a.</td>
</tr>
<tr>
<td>20</td>
<td>2^2 · 5</td>
<td>Product of ≤ 3 primes</td>
<td>50</td>
<td>2 · 5^2</td>
<td>Product of ≤ 3 primes</td>
</tr>
<tr>
<td>21</td>
<td>3 · 7</td>
<td>Product of ≤ 3 primes</td>
<td>51</td>
<td>3 · 17</td>
<td>Product of ≤ 3 primes</td>
</tr>
<tr>
<td>22</td>
<td>2 · 11</td>
<td>Product of ≤ 3 primes</td>
<td>52</td>
<td>2^2 · 13</td>
<td>Product of ≤ 3 primes</td>
</tr>
<tr>
<td>23</td>
<td>23</td>
<td>Part a.</td>
<td>53</td>
<td>2 · 3^3</td>
<td>See below</td>
</tr>
<tr>
<td>24</td>
<td>2^3 · 3</td>
<td>See below</td>
<td>54</td>
<td>2 · 3^3</td>
<td>Product of ≤ 3 primes</td>
</tr>
<tr>
<td>25</td>
<td>5^2</td>
<td>Part a.</td>
<td>55</td>
<td>5 · 11</td>
<td>See below</td>
</tr>
<tr>
<td>26</td>
<td>2 · 13</td>
<td>Product of ≤ 3 primes</td>
<td>56</td>
<td>2^3 · 7</td>
<td>Product of ≤ 3 primes</td>
</tr>
<tr>
<td>27</td>
<td>3^3</td>
<td>Product of ≤ 3 primes</td>
<td>57</td>
<td>3 · 19</td>
<td>Product of ≤ 3 primes</td>
</tr>
<tr>
<td>28</td>
<td>2^2 · 7</td>
<td>Product of ≤ 3 primes</td>
<td>58</td>
<td>2 · 29</td>
<td>Product of ≤ 3 primes</td>
</tr>
<tr>
<td>29</td>
<td>29</td>
<td>Part a.</td>
<td>59</td>
<td>7</td>
<td>Part a.</td>
</tr>
<tr>
<td>30</td>
<td>2 · 3 · 5</td>
<td>Product of ≤ 3 primes</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
</tbody>
</table>

By what we are allowed to assume, we see that we need only handle a few specific cases to complete the proof. We handle the cases in order from least to greatest so that, in each case, it suffices to show that a group $G$ of that order is not simple. In such a case, its nontrivial normal subgroup $N$ will be solvable (as it has order less than the given group), as will the quotient $G/N$, thus implying that $G$ is solvable. In each, case $n_p$ denotes the number of Sylow $p$-subgroups and Syl(G) denotes the set of Sylow $p$-subgroups of $G$.

Case 1, $|G| = 24$: If $|G| = 24$, then Sylow’s Theorems imply that $n_2 = 1$ or 3 and $n_3 = 1, 4, 8$. If $n_3 = 1$, we are done; suppose then that $n_2 = 3$. Let $G$ act on Syl(G) via conjugation, and denote this action via the homomorphism $\pi: G \to \text{Perms(Syl}_2(G)) \cong S_3$. Then $|G| = 24$ and $|S_3| = 3! = 6$. As the action is transitive, $\ker \pi G$, but since $G/\ker \pi$ is
isomorphic to a subgroup of $S_3$, we must have that $|G|/|\ker \pi| \leq 6$, so that $|\ker \pi| \geq 4$. Therefore, $G$ is not simple, hence is solvable. √

Case 2, $|G| = 36$: In this case, we see that $n_2 = 1, 3, 9$, and $n_3 = 1$ or 4. If $n_3 = 1$, we are done, and if not, $n_3 = 4$. If this is the case, let $G$ act on $\text{Syl}_3(G)$ via conjugation; we get a map $\pi : G \to \text{Perms}(\text{Syl}_3(G)) = S_4$. Again, this action is transitive, so $\ker \pi \neq G$. Moreover, $G/\ker \pi$ is isomorphic to a subgroup of $S_4$, and as $|S_4| = 4! = 24$, we find that $|G|/|\ker \pi| \leq 24$, i.e., $|\ker \pi| \geq 3$. Thus, $\ker \pi \cong G$, so $G$ is not simple, and hence $G$ is solvable. √

Case 3, $|G| = 40$: In this case, we see from Sylow’s Theorems that $n_5 = 1$, so the Sylow 5-subgroup $P_5$ is normal in $G$, whence $G$ is not simple, thus solvable. √

Case 4, $|G| = 48$: If $|G| = 48$, $n_2 = 1$ or 3, and $n_3 = 1, 4$, or 16. If $n_2 = 1$, we are done. If not, let $G$ act on $\text{Syl}_2(G)$ by conjugation. In doing so, we produce a nontrivial homomorphism $\pi : G \to \text{Perms}(\text{Syl}_2(G)) = S_3$. As in Case 1, we find that $\ker \pi$ is a nontrivial normal subgroup of $G$, whence $G$ is not simple. Consequently, $G$ is solvable. √

Case 5, $|G| = 54$: If $|G| = 54$, we see that $n_3 = 1$. Thus, the Sylow 3-subgroup of $G$ is normal, implying that $G$ is solvable. √

Case 6, $|G| = 56$: If $|G| = 56$, we see that $n_2 = 1$ or 7, and $n_7 = 1$ or 8. Assume $n_7 \neq 1$, i.e., $n_7 = 8$ (if $n_7 = 1$, then we are done). Then we find $6 \cdot 8 = 48$ distinct elements of $G$ having order 7 (six in each of the eight assumed Sylow 7-subgroups). Notice that any Sylow 2-subgroup of $G$ has 8 elements; therefore, there can only be one, as $G$ has 48 elements of order 7. Thus, the Sylow 2-subgroup is normal, whence $G$ is solvable. √

**Question 3.** Find all integers $0 < n < 20$ such that there exists a non-nilpotent group of order $n$. Justify your answer.

(You may assume whatever general facts you know about nilpotent groups, but explicitly state any fact you use. If you claim a particular group is or is not nilpotent, either give a proof or cite a general fact that justifies your claim.)

**Claim:** The set of $n$ with $0 < n < 20$ such that there is a non-nilpotent group of order $n$ is $\{6, 10, 12, 14, 18\}$.

**Proof.** Throughout, we make repeated use of the fact that a finite group $G$ is nilpotent if and only if it is isomorphic to a direct product of its Sylow subgroups. In particular, each group having prime power order is isomorphic to a direct product of its Sylow subgroups, and so is nilpotent. Using this fact alone, we need only consider the cases of groups with orders 6, 10, 12, 14, 15, and 18.

**Case 1, $|G| = 6$:** Consider the group $G = S_3$. The Sylow subgroups of $S_3$ are cyclic of orders 2 and 3, denoted $C_2$ and $C_3$, respectively. But $C_2 \times C_3 = C_6$ by the Chinese Remainder Theorem, and $S_3$ is not cyclic, so $S_3$ is not isomorphic to $C_6$. Thus, $S_3$ is not nilpotent.

**Case 2, $|G| = 10$:** Consider the group $G = D_{10}$, the symmetries of the regular pentagon. The Sylow subgroups of $G$ are $C_2$ and $C_5$, and $C_2 \times C_5 \cong C_{10}$. But $G$ is not cyclic, so $G$ is not isomorphic to a direct product of its Sylow subgroups, so $G$ is not nilpotent.

**Case 3, $|G| = 12$:** Consider the group $G = A_4$, a nonabelian group of order 12. Its Sylow 2-subgroups have order 4, and thus are isomorphic to $C_2 \times C_2$ or $C_4$, and its Sylow 3-subgroup is cyclic of order 3. In either case, the direct product of its Sylow subgroups is abelian, so is not isomorphic to $G$. Consequently, $G$ is not nilpotent.

**Case 4, $|G| = 14$:** Consider the group $G = D_{14}$, the symmetries of the regular heptagon. Its Sylow subgroups are $C_2$ and $C_7$, cyclic of orders 2 and 7, respectively. Now, $C_2 \times C_7 \cong C_{14}$, which is not isomorphic to $G$. Thus, $G$ is not nilpotent.

**Case 5, $|G| = 15$:** Let $G$ be a group of order 15. Then $G$ has unique Sylow subgroups $P_3$ and $P_5$, each of which is cyclic of orders 3 and 5, respectively. Moreover, $P_3 \cap P_5 = \langle e \rangle$, so $G \cong P_3 \rtimes \phi P_5$ for some $\phi : P_5 \to \text{Aut}(P_3) \cong C_2$. However, the only such $\phi$ is trivial, hence $G = P_3 \rtimes P_5$, and so $G$ is nilpotent. Thus, all groups of order 15 are nilpotent.

**Case 6, $|G| = 18$:** Let $G$ be $D_{18}$, the group of symmetries of the regular 9-gon. Let $P_3$ and $P_5$ be Sylow 2- and 3-subgroups of $G$. Then $P_2$ is cyclic of order 2, and $P_3 \cong C_3 \times C_3$ or $C_9$. In either case, $P_2 \times P_3$ is abelian, so is not isomorphic to $G$. Thus, $G$ is not nilpotent. ■
**Question 4.** Let $F/k$ be an extension of fields such that $|k| = 3^6$ and $|F| = 3^{60}$. How many elements $a \in F$ are there with $k(a) = F$? Justify your answer.

**Answer:** There are $3^{60} - 3^{30} - 3^{12} + 3^6$ elements $a \in F$ such that $k(a) = F$.

**Proof.** First, recall a few fundamental facts about finite fields and the structure of finite field extensions:

- Given a prime $p$ and positive integer $n$, there is a unique finite field of order $p^n$.
- If $E$ is a finite field, then $|E| = p^k$ for some prime $p$ and positive integer $k$.
- Let $L_1$ and $L_2$ be finite fields of orders $p^m$ and $p^n$, respectively. Then $L_1 \subseteq L_2$ if and only if $m|n$.
- Every finite extension of a finite field is separable.

**Terminology:** Given a field extension $F/k$ and an element $a \in F$, by the degree of $a$ over $k$ we mean $\deg f_{a,k}$, i.e., the degree of the minimal polynomial of $a$ over $k$ (and thus, $[k(a) : k]$).

Now, on to the proof. Notice that $[F : k] = 10$; thus, $a \in F$ gives $k(a) = F$ if and only if $a$ has degree 10 over $k$ (to use the terminology just defined), since there is a unique finite field of degree 10 over $k$. Using the facts above, let $E_1$ be the unique finite field of order $3^{12}$ and $E_2$ be the unique finite field of order $3^{30}$, so that $[E_1 : k] = [F : E_2] = 2$ and $[F : E_1] = [E_2 : k] = 5$. We get a subfield lattice:

```
  F
 /\  /
E_1 \ E_2
 /  /
 k 2
```

Now, no $\beta \in E_1 \cup E_2$ gives $k(\beta) = F$, as elements of $E_1 \cup E_2$ have degree 1, 2, or 5 over $k$. Moreover, if $\beta \in F \setminus (E_1 \cup E_2)$, then $k(\beta) = F$, since $k \subseteq k(\beta) \subseteq F$, and $E_1$ and $E_2$ are the only proper intermediate fields of the extension $F/k$ (but $\beta \notin E_1 \cup E_2$, so $k(\beta) \neq E_i$ for $i = 1, 2$). Thus, the set of primitive generators of $F/k$ is $F \setminus (E_1 \cup E_2)$, so it suffices to find the cardinality of this set. Notice that $E_1 \cap E_2 = k$, for if $\gamma \in E_1 \cap E_2$, then $k \subseteq k(\gamma) \subseteq E_i$ for each $i$, thus implying that $[k(\gamma) : k]$ divides both 2 and 5, hence must be 1. Thus, $\gamma \in E_1 \cap E_2$ implies $\gamma \in k$, and since $k \subset E_1 \cap E_2$ we find $k = E_1 \cap E_2$. Thus, $|E_1 \cup E_2| = |E_1| + |E_2| - |E_1 \cap E_2| = 3^{12} + 3^{30} - 3^6$, so the number of primitive generators of $F/k$ is $3^{60} - 3^{30} - 3^{12} + 3^6$, as claimed.

**Question 5.** Let $F$ be a finite (but not necessarily Galois) extension of a field $K$. Given a subgroup $G < \text{Aut}_K(F)$, let $F^G$ denote the intermediate field $\{f \in F : g(f) = f \text{ for all } g \in G\}$.

a. Let $G < \text{Aut}_K(F)$ be a subgroup. Prove Artin’s theorem that $F/F^G$ is a finite Galois extension with Galois group $G$.

**Proof.** Let $a \in F \setminus K$, and $G\alpha = \{\alpha, \cdots, \alpha_r\}$ be the distinct elements of the orbit of $\alpha$ under $G$. Let $f(x) = \prod_{i=1}^r (x - \alpha_i)$.

The action of $G$ on $F$ extends to an action of $G$ on $F[x]$ by defining $g \cdot x = x$ for all $g \in G$. In particular,

$$g(f(x)) = g \left( \prod_{i=1}^r (x - \alpha_i) \right) = \prod_{i=1}^r (x - g\alpha_i) = f(x),$$

as $g$ permutes the $\alpha_i$’s. Therefore, the coefficients of $f(x)$ are fixed by $G$, whence $f(x) \in K[x]$. Thus, $f_{\alpha,K}|f$, so in particular, $\alpha$ is separable and algebraic over $K$. We also have that $F/K$ is normal, as, given any $\beta \in F$, the roots of $f_{\beta,K}$ are among the elements of $G\beta$. As $F/K$ is finite, we conclude that $F/K$ is Galois. Moreover, $G \subseteq \text{Aut}_K(F)$. By Theorem 9 on pp. 570 of Dummit and Foote, $|F : K| = |G| \leq |\text{Aut}_K(F)| = |F : K|$, so we see $|G| = |\text{Aut}_K(F)|$, and thus $G = \text{Aut}_K(F)$.

b. Let $S$ be the set of subgroups of $\text{Aut}_K(F)$ and let $I$ be the set of intermediate fields of the extension. Define a map $\varphi : S \to I$ for any $G \in S$ by setting $\varphi(G) = F^G$. Show that $\varphi$ is always injective and give an example to show that $\varphi$ need not be surjective.
Question 6. Determine Aut(R).

Claim: \( \text{Aut}(R) = (\text{id}_R). \)

Proof. Recall first, that if \( a \in \mathbb{R} \) and \( a > 0 \), we have the existence of some \( b \in \mathbb{R} \) for which \( a = b^2 \). Thus, if \( \sigma \in \text{Aut}(R) \), we see that \( \sigma(a) = \sigma(b^2) = \sigma(b)^2 > 0 \). Thus, if \( x, y \in \mathbb{R} \) with \( x - y > 0 \), we see that \( \sigma(x) - \sigma(y) = \sigma(0) \). So \( \sigma(x) > \sigma(y) \). Thus, any field automorphism of \( \mathbb{R} \) is strictly increasing. Now, notice that, if \( m \in \mathbb{Z} \) and \( m \geq 0 \), as \( \sigma(1) = 1 \) we have that \( \sigma(m) = \sigma(1) + \sigma(1) + \cdots + \sigma(1) = 1 + 1 + \cdots + 1 = m \). If \( m \leq 0 \) and \( m \in \mathbb{Z} \), we see that \( \sigma(-m) = -m \), so \( -\sigma(-m) = \sigma(m) = m \), proving that \( \sigma \) fixes \( \mathbb{Z} \). Given any \( x \in \mathbb{Q} \), \( x = m/n = mn^{-1} \), so we see that \( \sigma(x) = \sigma(m/n) = \sigma(m)\sigma(n^{-1}) = mn^{-1} = mn/n = x \). Thus, \( \sigma \) fixes all rationals. Next, we notice that \( \sigma \) must be continuous, for if \( x \in \mathbb{R} \) and \( n \in \mathbb{N} \), we find that for any \( y \) such that \(-1/n < x - y < 1/n\) we have \( \sigma(-1/n) = -1/n < \sigma(x - y) = \sigma(x) - \sigma(y) \). Thus, \( \sigma(1/n) = 1/n \), proving that \( \sigma \) is continuous. Finally, let \( \lambda \in \mathbb{R} \setminus \mathbb{Q} \). Then \( \lambda \) has a decimal expression \( \lambda = d_0.d_1d_2\cdots \). Given \( n \in \mathbb{N} \), define a sequence \( (a_n)_{n=0}^{\infty} \) by \( a_n = d_0.d_1\cdots d_n \). Then \( (a_n) \in \mathbb{Q} \) converges to \( \lambda \), and as \( \sigma \) is continuous, \( \sigma(\lambda) = \lim_{n \to \infty} \sigma(a_n) = \lim_{n \to \infty} a_n = \lambda \). Thus, \( \sigma \) fixes every real number, hence \( \sigma = \text{id}_R \), and the claim follows.

Part III: Rings and Modules

Question 7. Let \( G \) be a finite group and let \( \mathbb{C} \) denote the field of complex numbers. Show that \( R = \mathbb{C}[G] \) has a nonzero nilpotent element if and only if \( G \) is a nonabelian group.

Proof. Let \( G \) be a finite group, and suppose instead that \( G \) is abelian. We show that \( \mathbb{C}[G] \) is nonabelian. By Maschke’s Theorem, \( \mathbb{C}[G] \) is semisimple, and by Wedderburn’s Theorem, \( \mathbb{C}[G] \cong \bigoplus_{i=1}^{r} M_{n_i}(\mathbb{C}) \) via an isomorphism \( \varphi \). But, if \( G \) is abelian, then \( \mathbb{C}[G] \) is commutative, and so we must have \( n_i = 1 \) for all \( i \). Suppose \( a \in \mathbb{C}[G] \) is nilpotent, i.e., there is an \( n \in \mathbb{N} \) for which \( a^n = 0 \). Then \( 0 = \varphi(a^n) = \varphi(a)^n \), so \( \varphi(a) \) is a nilpotent element of \( \bigoplus_{i=1}^{r} \mathbb{C} \), i.e., \( \varphi(a) = (a_1, \ldots, a_r) \), we have \( a_i^n = 0 \) for each \( i \). As \( \mathbb{C} \) is a field, \( a_i = 0 \) for each \( i \), so \( a = 0 \). Thus, \( \mathbb{C}[G] \) has no nonzero nilpotents. Conversely, if \( G \) is nonabelian, then \( \mathbb{C}[G] \) is non-commutative, so by the theorems of Maschke and Wedderburn, \( \mathbb{C}[G] \cong \bigoplus_{i=1}^{r} M_{n_i}(\mathbb{C}) \) via an isomorphism \( \varphi \), and as \( \mathbb{C}[G] \) is non-commutative, there is an \( i_0 \) for which \( n_{i_0} > 1 \). Let \( a \) be the element of \( \mathbb{C}[G] \) corresponding via \( \varphi \) to the element \((0,0,\cdots,0,0,\cdots,0)\), where \( A = \begin{bmatrix} 0 & i \\ 0 & 0 \end{bmatrix} \), i.e., the matrix which is 0 everywhere except the \( n_{i_0} \)th entry of the first row, which has entry \( i \). However, since \( A \neq 0 \), \( a \neq 0 \), and as \( A^2 = 0 \), we find that \( a^2 = 0 \). Thus, \( \mathbb{C}[G] \) has a nonzero nilpotent.

Question 8. Let \( A \) be a commutative ring with \( 1 \neq 0 \). Let \( M \) and \( N \) be \( A \)-modules. Show that \( M \oplus N \) is flat if and only if \( M \) and \( N \) are flat.

Proof. We begin by proving a claim, using the following version of the Universal Property of the Tensor Product: given any \( A \)-modules \( B, C \) and \( S \), there is an \( A \)-bilinear map \( \varphi_{B,C} : B \times C \to P \otimes_A C \) such that any \( A \)-bilinear map \( B \times C \to S \) factors in a unique way through \( \varphi \).
Math 901-902       June 2009 Comprehensive Exam

Claim: If $M, N, B$ are $A$-modules, then $B \otimes (M \oplus N) \cong (B \otimes M) \oplus (B \otimes N)$.

Proof of Claim: First define a map $B \times (M \oplus N) \to (B \otimes M) \oplus (B \otimes N)$ by

$F((b, (m, n))) = (b \otimes m, 0)$. This is bilinear, so there is a unique homomorphism $f : B \otimes (M \oplus N) \to (B \otimes M) \oplus (B \otimes N)$ such that $F = f \otimes_{B, \mathbb{M} \oplus \mathbb{N}}$. Likewise we have a bilinear map $G : B \times (M \oplus N) \to (B \otimes M) \oplus (B \otimes N)$ and the homomorphism $g : B \otimes (M \oplus N) \to (B \otimes M) \oplus (B \otimes N)$ with $G = g \otimes_{B, \mathbb{M} \oplus \mathbb{N}}$. We now obtain a homomorphism $f + g : B \otimes (M \oplus N) \to (B \otimes M) \oplus (B \otimes N)$ by addition in the target. On a simple tensor we have $(f + g)(b \otimes (m, n)) = (b \otimes m, b \otimes n)$.

On the other hand, we have bilinear maps $H_M : B \times M \to B \otimes (M \oplus N)$ and $H_N : B \times N \to B \otimes (M \oplus N)$ defined as $H_M((b, m)) = b \otimes (m, 0)$ and $H_N((b, n)) = b \otimes (0, n)$. These induce $A$-module homomorphisms $h_M : B \otimes M \to B \otimes (M \oplus N)$ and $h_N : B \otimes N \to B \otimes (M \oplus N)$, which together induce $h_M \oplus h_N : (B \otimes M) \oplus (B \otimes N) \to B \otimes (M \oplus N)$. We have $h_M \oplus h_N((b \otimes m, b \otimes n)) = h_M(b \otimes m) + h_N(b \otimes n) = (b \otimes (m, 0)) + (b \otimes (0, n)) = (b, m, n)).$

Since elements of the form $(b \otimes (m, n))$ generate $B \otimes (M \oplus N)$ and since $(h_M \oplus h_N)((f + g)(b \otimes (m, n))) = b \otimes (m, n)$, we see $(h_M \otimes h_N)(f + g) = (f + g)(b \otimes (m, n)) = b \otimes (m, n)$ and $h_M \oplus h_N = (f + g)(b \otimes (m, n)) = (b, m, n))$. This is the identity. √

Now suppose first that $B \otimes C \overline{\otimes} D$ is exact, and that $M$ and $N$ are both flat. This implies that $B \otimes M \underset{f \otimes 1_M}{\overset{g \otimes 1_M}{\longleftarrow}} C \otimes M \underset{g \otimes 1_M}{\overset{f \otimes 1_M}{\longrightarrow}} D \otimes M$ is exact, as is $B \otimes N \underset{f \otimes 1_N}{\overset{g \otimes 1_N}{\longleftarrow}} C \otimes N \underset{g \otimes 1_N}{\overset{f \otimes 1_N}{\longrightarrow}} D \otimes N$. But these are exact if and only if

$$\frac{(B \otimes M) \oplus (B \otimes N)}{(f \otimes 1_M)(g \otimes 1_N)(C \otimes M)(C \otimes N)} \cong \frac{(D \otimes M) \oplus (D \otimes N)}{(g \otimes 1_M)(f \otimes 1_M)(C \otimes M \oplus C \otimes N)}$$

is exact. By the isomorphism established above, (1) is exact if and only if

$$\frac{(B \otimes (M \oplus N))}{(f \otimes 1_{M \oplus N})(g \otimes 1_{M \oplus N})(C \otimes (M \oplus N))} \cong \frac{(D \otimes (M \oplus N))}{(g \otimes 1_{M \oplus N})(f \otimes 1_{M \oplus N})(C \otimes (M \oplus N))}$$

is exact. Therefore, $M \oplus N$ is flat if and only if $M$ and $N$ are flat.

---

Question 9. Compute the number of elements in the $\mathbb{Z}$-module $A \otimes \mathbb{Z} \text{Hom}_\mathbb{Z}(M \oplus N, P \oplus Q)$, where $A = \mathbb{S}^{-1}\mathbb{Z}$, $\mathbb{S} = \{1, 5, 5^2, \ldots\}$, $M = \mathbb{Z}/9\mathbb{Z}$, $N = \mathbb{Z}/5\mathbb{Z}$, $P = \mathbb{Z}/3\mathbb{Z}$, and $Q = \mathbb{Z}/25\mathbb{Z}$. Justify your answer.

Claim: $|A \otimes \mathbb{Z} \text{Hom}_\mathbb{Z}(M \oplus N, P \oplus Q)| = 3$.

Proof. Notice that $M \oplus N = \mathbb{Z}_{45} = \langle a \rangle$, the cyclic group of order 45, written additively. Similarly, $P \oplus Q = \mathbb{Z}_{75} = \langle b \rangle$, the cyclic group of order 75, written additively. Given $\varphi \in \text{Hom}_\mathbb{Z}(\mathbb{Z}_{45}, \mathbb{Z}_{75})$, we notice that $\varphi$ is completely determined by $\varphi(a)$. We adopt the following terminology: if $\varphi \in \text{Hom}_\mathbb{Z}(\mathbb{Z}_{45}, \mathbb{Z}_{75})$, then by the order of $\varphi$ (written $o(\varphi)$), we mean $|\varphi(a)|$ in $\mathbb{Z}_{75}$. The order of $\varphi$ must divide both 45 and 75, and so we have the following possibilities: $o(\varphi) = 1, 3, 5, 15$. We find

Case 1: If $o(\varphi) = 1$, then $\varphi(x) = 0$ for every $x \in \mathbb{Z}_{45}$, and hence for any $a \in A$, $a \otimes \varphi = 0$.

Case 2: If $o(\varphi) = 3$, then $\varphi(a) = 25b$ or $50b$. Notice that, if $\varphi(a) = 25b$, then $5 \cdot \varphi(a) = 50b$ and if $\varphi(a) = 50b$, then $5 \cdot \varphi(a) = 25b$.

Case 3: If $o(\varphi) = 5$, then $\varphi(a) = 15b$, $30b$, $45b$, or $60b$. Since $5j = 0$ in $\mathbb{Z}_{75}$ (for any $j \in \{15, 30, 45, 60\}$), so $\frac{x}{5m} \otimes \varphi = \frac{x}{5m+1} \otimes \varphi = \frac{x}{5m+1}$ and $\varphi = 0$.

Case 4: If $o(\varphi) = 15$, then $\varphi(a) = (5kb : k \in \mathbb{N}, 1 \leq k \leq 14)$. One may check that, in each case, either $5\varphi \equiv 0$ or $o(5\varphi) = 3$. Thus, if $\varphi$ has order 15 and $x \in A$, $x \otimes \varphi = x/5 \otimes \varphi = 0$ or $\varphi$ has order 3, reducing to Case 2.

Thus, given $x \otimes \psi$ in the module in question, there are three possibilities for $\psi$: call them $\psi_1, \psi_2,$ and $\psi_3$, where $\psi_1 \equiv 0$ and $\psi_2, \psi_3$ have order 3. Let $m \in \mathbb{N}$. Then $1 \otimes \psi_1 \equiv 5^m/5^m \otimes \psi_1 \equiv 1/5^m \otimes 5^m \psi_1 \equiv 1/5^m \otimes \psi_j$ for some $j \in \{1, 2, 3\}$. Now, by work done in Case 2, $\psi_2 = 5\psi_3$ and $\psi_3 = 5\psi_2$. Therefore, given $n \in \mathbb{N}$ and $i \in \{2, 3\}$, $5^m \otimes \psi_i \equiv 1 \otimes \psi_i$ if $n$ is even and $1/5^m \otimes \psi_i \equiv 1 \otimes \psi_i$ if $n$ is odd. Moreover, if $a \in A$, then $a = b/5^m$ for some $m$, and we see $b/5^m \otimes \psi_i \equiv 1/5^m \otimes \psi_i$. If this simple tensor is not zero, then $b \psi_i \equiv \psi_2, \psi_3$, so $a \otimes \psi_1 \equiv 5^m \otimes \psi_1 \equiv 1 \otimes \psi_k$ for $i, j, k \in \{2, 3\}$. Thus, we may write $\sum_{j=1}^{15} \sigma_j \otimes \psi_i = \sum_{j=1}^{15} \sigma_j \otimes \psi_i \equiv \sum_{j=1}^{15} \sigma_j \otimes \psi_i$, where $\sigma_1, \psi_i \in \psi_1, \psi_2, \psi_3$ for $i$. Therefore, each element of the module is a simple tensor $x \otimes \gamma$ with $x \in \{0, 1, 1/1\}$ and $\gamma \in \{\psi_1, \psi_2, \psi_3\}$. When we count the options, we find the claim proved.