Mathematics GU4044 Representations of Finite Groups
Assignment # 8

Benjamin Church

April 2, 2018

Problem 1.

(a). Let G be a finite group with even order. Let $X \subset G$ be the set of elements of order greater than 2. For each $x \in X$ we know that $x^{-1} \in X$ since $\text{ord}(x) = \text{ord}(x^{-1})$. However, if $x = x^{-1}$ then $x^2 = e$ so $ord x \le 2$ and thus $x \notin X$. Therefore, X is even because x and x^{-1} are not equal and inverses are unque so X splits up into pairs. Therefore, $G - X$ has at least two elements because $\#(G)$ and $\#(X)$ are even so $\#(G - X)$ is even but $e \in G - X$ so there must be at least two elements in $G - X$.

(b). Let $\#(G) = 2a$ such that $a > 1$ is odd. Consider the homomorphism $f : G \to S_G \cong S_{2a}$ defined by the action of G on itself by left multiplication. If $g \in G$ has order 2 then consider the permutation corresponding to the action $g \cdot h = gh$. If $gh = h$ then $g = e$ contradicting g having order 2. Therefore, g must swap pairs of elements since $g^2 = e$ so $g \cdot (g \cdot h) = h$. Therefore, $f(g)$ is the product of a disjoint 2-cycles so $f(g)$ is odd since a is odd. Now, consider the subgroup $f^{-1}(A_{2a}) \lhd G$ which is normal because $A_{2a} \lhd S_{2a}$. However, by part (i) G has at least two elements of order 2. For each such g, we know that $f(g) \notin A_{2a}$ since it is an odd permutation. Thus, $f^{-1}(A_{2a}) \neq G$. Furthermore, for any $g \in G$ we know that $f(g^2) = f(g)^2 \in A_{2a}$ but if $a > 1$ then there must exist nontrival squares in G else the order of every element would be 2 implying that there are no Sylow p-groups for any $p \neq 2$ which cannot be possible since $a > 1$ is odd and therefore must have an odd prime factor. Thus, $f^{-1}(A_{2a})$ contains some nontrivial element so $f^{-1}(A_{2a})$ is a nontrivial proper normal subgroup so G is not simple.

Problem 2.

Let p and q be primes with $p < q$ with $q \equiv 1 \mod p$. Let G be a non-abelian group of order pq. We know by Frobenius that the dimension of any irreducible representation is one of $1, p, q, pq$. Furthermore, the dimensions sum,

$$\sum_{i=1}^{h} d_i^2 = pq$$

Therefore, no irreducible representation can have dimension q or pq. Let c_1 be the number of 1-dimensional representations of G and c_p be the number of p-dimensional representations. Then,

$$c_1 + c_p p^2 = pq \implies p \mid c_1$$

Therefore, $c_1 = pk$. However, $c_1 = \#(G^{ab})$ which divides $\#(G)$. Thus, $c_1 = p$ or $c_1 = pq$. If $c_1 = pq$ then $c_p = 0$ and thus G is abelian. Otherwise, $c_1 = p$ and $1 + c_p p = q$. Since G is non-abelian, we have $c_1 = p$ and $c_p = \frac{1}{p}(q-1)$. Furthermore, the number of conjugacy classes is equal to the number of irreducible representations, $h = c_1 + c_p = p + \frac{1}{p}(q-1)$.

Problem 3.

Let G be a finite group with $\#(G) = p^a$. By Frobenius' theorem, we know that $d_i \mid p^a$ so $d_i = p^{k_i}$ for each irreducible representation. Furthermore, we know that,

$$\sum_{i=1}^{h} d_i^2 = \sum_{i=1}^{h} p^{2k_i} = p^a$$

For any irreducible representation of dimension greater than one, $p \mid d_i$ so if c_1 is the number of 1-dimensional representations then $p \mid c_1$ since,

$$c_1 = p^a - \sum_{d_i > 1} p^{2k_i}$$

Therefore, there must be a nontrivial G-representation of dimension 1 and thus a nontrivial homomorphism $\lambda : G \to \mathbb{C}^\times$ but $\mathbb{C}^\times$ is an abelian group so $\ker \lambda \supset G'$ but $\ker \lambda \neq G$ since λ is nontrivial. Thus, $G' \neq G$. Furthermore, either $G' = \{e\}$ and then all comutators vanish so G is abelian or $G' \neq \{e\}$. Thus, if G is nonabelian then G' is a nontrivial proper normal subgroup. Therefore, if G is simple then G must be abelian and thus must have no nontrivial subgroups with implies that the order of every element is either 1 or $\#(G)$ so G is cyclic of prime order. Clearly, for the converse, any group with $\#(G) = p$ is cyclic because $\mathrm{ord}(x) \mid p$ so $\mathrm{ord}(x) = p$ for nontrivial x and thus G is cyclic of prime order and then simple.

Problem 4.

Let d be an integer non equal to ± 1 which is square-free. Let $K = \mathbb{Q}(\sqrt{d})$. Consider the element $\alpha = r + s\sqrt{d}$. We know that α is a root of the polynomial,

$$f(x) = (x - \alpha)(x - \bar{\alpha}) = x^2 - (\alpha + \bar{\alpha})x + \alpha\bar{\alpha} = x^2 - 2r + r^2 - s^2 d$$

Therefore, if $2r$ and $r^2 - s^2 d$ are integers then α is an algebraic integers. Thus, if $r, s \in \mathbb{Z}$ then α is an algebraic integer. Furthermore, if $d \equiv 1 \bmod 4$, and $\alpha \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ then $r = a + \frac{1}{2}b$ and $s = \frac{b}{2}$ for $a, b \in \mathbb{Z}$. Then, $2r = 2a + b \in \mathbb{Z}$ and $r^2 - s^2 d = a^2 + ab + \frac{b^2 - b^2 d}{4} = a^2 + ab + b^2 \frac{1-d}{4} \in \mathbb{Z}$ because $d \equiv 1 \bmod 4$. Therefore, $\mathbb{Z}[\sqrt{d}]$ are all algebraic integers and for $d \equiv 1 \bmod 4$ the set $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ are all algebraic integers.

Furthermore, we know that $\alpha, \bar{\alpha} \in \mathbb{C}$ are algebraic integers. Therefore, $\alpha + \bar{\alpha} = 2r$ is an algebraic integer and a rational and thus an integer. Likewise, $\alpha\bar{\alpha} = r^2 - s^2 d$ is an algebraic integer and is rational and thus is an integer. Therefore, $r = \frac{a}{2}$ where $a \in Z$ which implies that $s^2 d = b + \frac{a^2}{4}$ for $b \in \mathbb{Z}$. Thus, $(2s)^2 d = b + a^2$ so $(2s)^2 d \in \mathbb{Z}$ which implies that $2s$ is an integer because d is squarefree so any denominator of $(2s)^2$ cannot divide d. Now we will analyize the following cases, $r = n + \frac{1}{2}$ and $s = m + \frac{1}{2}$ for $n, m \in \mathbb{Z}$. Then,

$$\left(n + \frac{1}{2}\right)^2 - \left(m + \frac{1}{2}\right)^2 d = n^2 + n + \frac{1}{4} - (m^2 - m - \frac{1}{4})d = n^2 + n - m^2 d - md + \frac{1-d}{4} \in \mathbb{Z}$$

Therefore $d \equiv 1 \bmod 4$. Next case, $r = n$ and $s = m + \frac{1}{2}$ for $n, m \in \mathbb{Z}$,

$$(n)^2 - \left(m + \frac{1}{2}\right)^2 d = n^2 - (m^2 - m - \frac{1}{4})d = n^2 - m^2 d - md - \frac{d}{4} \in \mathbb{Z}$$

which is impossible since d is squarefree. Next case, $r = n + \frac{1}{2}$ and $s = m$ for $n, m \in \mathbb{Z}$,

$$\left(n + \frac{1}{2}\right)^2 - (m)^2 d = n^2 + n + \frac{1}{4} - m^2 d = n^2 + n + \frac{1}{4} - m^2 d \in \mathbb{Z}$$

which is clearly impossible. Finally, if $r, s \in \mathbb{Z}$ then $r^2 - s^2 d \in \mathbb{Z}$ is clearly true. Therfore, we have shown that if α is an algebraic integer then $\alpha \in \mathbb{Z}[\sqrt{d}]$ unless $h \equiv 1 \bmod 4$ in which case $\alpha \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$.

Problem 5.

Consider the field $\mathbb{Q}(\sqrt{d})$. If $\alpha \in \mathbb{Q}(\sqrt{d})$ and α is an algebraic integer then if $d < 0$ then either $|\alpha| > 0$ or $\alpha = 0$. This is because $\bar{\alpha}$ is also an algebraic integer such that $\alpha\bar{\alpha}$ is a rational algebraic integer so $\alpha\bar{\alpha}$ is an integer. Therefore, $|\alpha| = \sqrt{\alpha\bar{\alpha}} \geq 1$ or $\alpha = 0$ since it is the square root of an integer. However, if $d > 0$ this may not be true. For example, consider $\alpha = 1 - \sqrt{2}$ which has absolute value less than one but positive.

Problem 6.

(a). Let G be a finite group and let C_1 and C_2 be two conjugacy classes in G. Consider,

$$\begin{aligned}(f_{C_1} * f_{C_2})(g) &= \sum_{xy=g} f_{C_1}(x) f_{C_2}(y) = \sum_{xy=g} \mathbf{1}_{(x \in C_1 \text{ and } y \in C_2)} \\ &= \#(\{(x,y) \in G \times G \mid xy = g\} \cap \{(x,y) \in G \times G \mid x \in C_1 \text{ and } y \in C_2\})\end{aligned}$$

which is the number of $(x, y) \in G \times G$ such that $xy = g$ and $x \in C_1$ and $y \in C_2$.

(b). The group S_3 has conjugacy classes,

$$C_1 = \{1\}, \quad C_2 = \{(1\,2), (1\,3), (2\,3)\}, \quad C_3 = \{(1\,2\,3), (1\,3\,2)\}$$

Define $f_{ij} = f_{C_i} * f_{C_j}$. Clearly, $f_{ij} = f_{ji}$. Furthermore, if $j = 1$ then $f_{i1}(g)$ is the number of $(x, y) \in G \times G$ such that $xy = g$ and $x \in C_i$ and $y \in C_1$ so $y = 1$ and then $x = g$ so there is exactly one solution if and only if $g \in C_i$ and none otherwise. Thus,

$$f_{i1}(g) = \begin{cases} 1 & g \in C_i \\ 0 & g \notin C_i \end{cases} = f_{C_i}$$

Therefore, we have determined f_{ij} except f_{22}, f_{23}, and f_{33}. Consider, $f_{22}(1) = 3$ because $(a\,b)^2 = e$. Next, the product of two 2-cycles is an even permutation and thus in $A_3 \cong \mathbb{Z}/3\mathbb{Z}$. Thus, $f_{22}(g) = 1$ if $g \in A_3$ and $f_{22}(g) = 0$ otherwise.

Next, $f_{33}(1) = 2$ because the three cycles are inverses. Furthermore, the product of any two three cycles is either a three cycle or 1. However, there is exacly one way to make any thee cycle from products of two of $(1\,2\,3)$ and $(1\,3\,2)$. Thus, $f_{33}(g) = 1$ if g is a three cycle and $f_{33}(g) = 0$ if g is not a three cycle or 1.

Finally, products of three cycles and two cycles are odd permutations and thus are 2-cycles. Given a 2-cycle g there are exactly two ways to make g as a product $x \in C_2$ and $y \in C_3$ as $(a\,b)(a\,b\,c) = (b\,c)$ and $(b\,c)(a\,c\,b) = (c\,b) = (b\,c)$. Therefore, $f_{23}(g) = 2$ if g is a 2-cycle and $f_{23}(g) = 0$ otherwise.