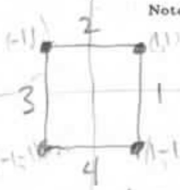
MAT 511 **HW #5** Name SOLUTIONS

10/13/13, due Friday 10/18/13

25 points

1. Use Burnside's Counting Formula to determine the number of different ways to color the four edges of a square using n colors, as a function of n, where two colorings are considered to be same if they become identical upon rotation or reflection of the square.

Note: There is a hint on the course web page.



Let Ω be the set of colorings of the labelled square; we can identify with the set of 4-tuples $\{(c_1,c_2,c_3,c_4) \mid 1 \le c_i \le n \text{ for } 1 \le i \le 4\}$. ($c_i$ = the color of edge i). Then $|\Omega| = n^4$. The dihedral group D_4 acts on Ω, and the "types" of colorings are the orbits. The numbers of fixed points of elements $g \in D_4$ are given in the following table. go to page 3

2. Let R be a ring, and M a left R-module. A *submodule* of M is a subgroup K of the underlying abelian group satisfying $r \cdot x \in K$ for every $x \in K, r \in R$. An R-*module homomorphism* $\varphi \colon M \to N$ of M to a left R-module N is a homomorphism of the underlying abelian groups satisfying $\varphi(r \cdot x) = r \cdot \varphi(x)$ for all $x \in M, r \in R$.

(a) Suppose K is a submodule of M. Show that the quotient abelian group M/K has a natural left R-module structure.

$M/K = \{x + K \mid x \in M\}$ is an abelian group (since $K \le M$) with $(x+K)+(y+K) = (x+y)+K$. Define "scalar multiplication" $\cdot : R \times M/K \to M/K$ by $r \cdot (x+K) = r \cdot x + K$, where $r \cdot x$ is the product in M. The product is well-defined: if $x+K = y+K$ then $x-y \in K$, and then $r \cdot (x-y) \in K$ because K is a submodule, and then $r\cdot x - r \cdot y \in K$, so $r \cdot x + K = r \cdot y + K$. Then the axioms are easily verified: $(r+s)\cdot(x+M) = (r+s)\cdot x + M = r\cdot x + s \cdot x + M = (r \cdot x + M) + (s \cdot x + M)$ and $r \cdot (s \cdot (x+M)) = r \cdot (s \cdot x + M) = r \cdot (s \cdot x) + M = (rs)\cdot x + M$. $r \cdot ((x+M)+(y+M)) = r \cdot (x+y+M) = r \cdot (x+y) + M = r \cdot x + r \cdot y + M = (r \cdot x + M) + (r \cdot y + M)$. □

(b) Suppose $\varphi \colon M \to N$ is an R-module homomorphism, which is an isomorphism of the underlying abelian groups. Prove that the set function $\varphi^{-1} \colon N \to M$ is an R-module homomorphism. (Thus φ is an isomorphism of left R-modules.)

Let $x, y \in N$. Let $u = \varphi^{-1}(x)$ and $v = \varphi^{-1}(y)$. Then $\varphi(u) + \varphi(v) = x + y$, and $\varphi(u) + \varphi(v) = \varphi(u+v)$, so $\varphi(u+v) = x+y$. Then $u + v = \varphi^{-1}(x+y)$. Thus $\varphi^{-1}(x+y) = \varphi^{-1}(x) + \varphi^{-1}(y)$. Also $\varphi(ru) = r\varphi(u) = rx$ so $ru = \varphi^{-1}(rx)$, hence $r\varphi^{-1}(x) = \varphi^{-1}(rx)$. Thus φ^{-1} is an R-module homomorphism.

(c) Suppose $\varphi \colon M \to N$ is an R-module homomorphism. Prove $\ker(\varphi)$ and $\operatorname{im}(\varphi)$ are submodules of M and N, respectively, and that φ induces an isomorphism of left R-modules $\overline{\varphi} \colon M/\ker(\varphi) \to \operatorname{im}(\varphi)$.

$\ker(\varphi) \le M$ by group theory, and $x \in \ker(\varphi)$, $r \in R \Rightarrow \varphi(rx) = r\varphi(x) = r \cdot 0_M = 0_M \Rightarrow rx \in \ker(\varphi)$. Thus $\ker(\varphi)$ is a submodule of M. $\operatorname{im}(\varphi) \le N$ by group theory. go to page 3.

3. Let R be a ring with 1 unital and M a left R-module. If $X \subseteq M$, the submodule generated by X is the intersection $\langle X \rangle$ of the family of submodules of M containing X.

(a) Prove $v \in \langle X \rangle$ if and only if $v = \sum_{x \in X} r_x \cdot x$, where $r_x \in R$ for every $x \in X$ and $r_x = 0_R$ for all but finitely many $x \in X$.

Since $X \subseteq \langle X \rangle$ and $\langle X \rangle$ is a submodule, $rx \in \langle X \rangle$ for all $x \in X$, $r \in R$, and any finite sum of such elements lies in $\langle X \rangle$, hence any $v = \sum_{x \in X} r_x x$ with only finitely many r_x nonzero lies in $\langle X \rangle$. Let N be the set of such v. Then $x = 1_R x \in N$ for all $x \in X$, and N is closed under $+$, $-$, and multiplication by $r \in R$, so N is a submodule of M. Then $\langle X \rangle \subseteq N$. Thus $\langle X \rangle = N$.

(b) A *basis* of an R-module M is a subset X of M satisfying $\langle X \rangle = M$ and

$$\sum_{x \in X} r_x \cdot x = 0_M \implies r_x = 0_R \text{ for all } x \in X,$$

for any collection $r_x \in R$, $x \in X$, satisfying $r_x = 0_R$ for all but finitely many $x \in X$. A left R-module is *free* if it has a basis. Prove that R^n, with its natural structure as a left R-module, is a free R-module.

Let $e_1 = (1_R, 0, \dots, 0)$, $e_2 = (0, 1_R, 0, \dots, 0)$, $\dots$ $e_i = (0, \dots, \underset{i}{1}, \dots, 0)$, $e_n = (0, \dots, 0, 1_R)$.

For any $x = (r_1, \dots, r_n) \in R^n$, $x = \sum_{i=1}^{n} r_i e_i$, so $\{e_1, \dots, e_n\}$ generates R^n. If $\sum_{i=1}^{n} r_i e_i = 0_{R^n}$, then $(r_1, \dots, r_n) = (0_R, \dots, 0_R)$, so $r_1 = r_2 = \dots = r_n = 0_R$. Thus $\{e_1, \dots, e_n\}$ is a basis of R^n, so R^n is a free R-module.

(c) Suppose M is a nontrivial finitely-generated left R-module, that is, $M = \langle X \rangle$ for some nonempty finite subset X of M. Prove that there is a surjective homomorphism $\varphi \colon R^n \to M$, for some $n \geq 1$, which is an R-module isomorphism if and only if X is a basis of M. [1]

Let $X = \{x_1, \dots, x_n\}$. Define $\varphi : R^n \to M$ by $\varphi((r_1, \dots, r_n)) = r_1 x_1 + \dots + r_n x_n$. It is straightforward to check that φ is an R-module homomorphism. φ is surjective since $\langle X \rangle = M$.

4. Suppose G is a finite group, and $|G| = \prod_{i=1}^{k} p_i^{n_i}$ is the prime factorization of $|G|$, with $p_1, \dots, p_k$ distinct primes and $n_i \geq 1$ for $1 \leq i \leq k$. Suppose H_i is a normal subgroup of G satisfying $|H_i| = p_i^{n_i}$ for $1 \leq i \leq k$. Prove G is isomorphic to the direct product $H_1 \times \cdots \times H_k$.

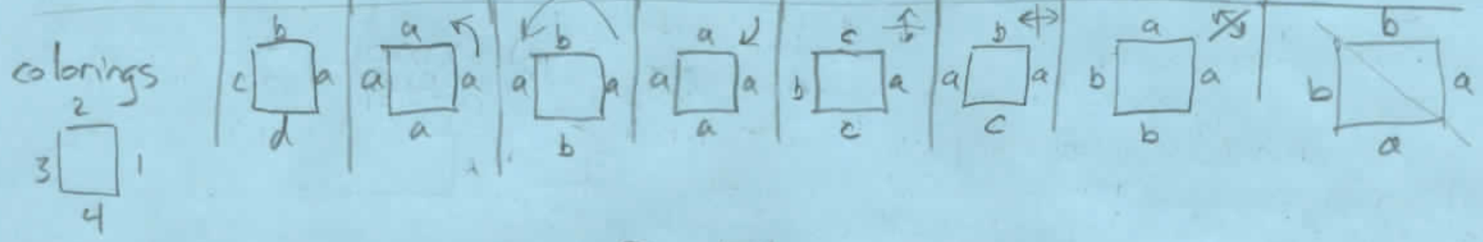
First, $H_i \cap (H_1 \cdots H_{i-1} H_{i+1} \cdots H_k) = 1$ because $H_i \cap (H_1 \cdots H_{i-1} H_{i+1} \cdots H_k)$ is a subgroup of H_i and of $H_1 \cdots H_{i-1} H_{i+1} \cdots H_k$, so its order divides $|H_i| = p_i^{n_i}$ and $|H_1 \cdots H_{i-1} H_{i+1} \cdots H_k|$, which divides $|H_1| \cdots |H_{i-1}| |H_{i+1}| \cdots |H_k| = p_1^{n_1} \cdots p_{i-1}^{n_{i-1}} p_{i+1}^{n_{i+1}} \cdots p_k^{n_k}$. Since the primes p_i are distinct, the intersection must be trivial. Then, arguing by induction,

[1] Once one proves that R^n is not isomorphic to R^m if $n \neq m$, then one can say "if and only if M is a free R-module," and define n to be the *rank* of the free R-module M.

$|H_1 \cdots H_k| = |H_1| \cdots |H_k| = p_1^{n_1} \cdots p_k^{n_k} = |G|$, so $H_1 \cdots H_k = G$. Since $H_i \trianglelefteq G$ for all i, this implies $G \cong H_1 \times \cdots \times H_k$.

① (continued)

matrix	$\begin{bmatrix}1&0\\0&1\end{bmatrix}$	$\begin{bmatrix}0&-1\\1&0\end{bmatrix}$	$\begin{bmatrix}-1&0\\0&-1\end{bmatrix}$	$\begin{bmatrix}0&1\\-1&0\end{bmatrix}$	$\begin{bmatrix}1&0\\0&-1\end{bmatrix}$	$\begin{bmatrix}-1&0\\0&1\end{bmatrix}$	$\begin{bmatrix}0&1\\1&0\end{bmatrix}$	$\begin{bmatrix}0&-1\\-1&0\end{bmatrix}$
induced permutation of edges	id	(1234)	(13)(24)	(1432)	(24)	(13)	(12)(34)	(14)(23)
# of fixed points	n^4	n	n^2	n	n^3	n^3	n^2	n^2



Then the number of orbits

$$N = \frac{1}{|G|}\sum_{g\in G}\chi(g) = \frac{1}{8}\left[n^4 + 2n^3 + 3n^2 + 2n\right].$$

e.g.

n	1	2	3	4	5	6	7
N	1	6	21	55	120	231	406

2(c) (continued) If $y \in \operatorname{im}(\varphi)$ and $r\in R$, then $y=\varphi(x)$ for some $x\in M$, and then $\varphi(rx) = r\varphi(x) = ry$, so $ry \in \operatorname{im}(\varphi)$. Thus $\operatorname{im}(\varphi)$ is a submodule of N.
By group theory, φ induces an isomorphism of groups $\overline{\varphi} : M/\ker(\varphi) \to \operatorname{im}(\varphi)$. Since $\overline{\varphi}(r\cdot(x+\ker(\varphi))) = \overline{\varphi}(rx+\ker(\varphi)) = \varphi(rx) = r\varphi(x) = r\overline{\varphi}(x+\ker(\varphi))$, so $\overline{\varphi}$ is an R-module isomorphism.