Blatt 6 - Solutions

1) a) To show that the operation defined in question 1 is associative is a straightforward calculation. The neutral element is $(1_N, 1_G)$ where 1_N and 1_G denote the neutral elements of N and G, respectively. For $(n,g) \in N \rtimes_c G$, the inverse of (n,g) equals $(c_{g^{-1}}(n^{-1}), g^{-1})$.

b) For only $c(g) = id_N$ $(g \in G)$ we have that $N \rtimes_c G$ equals the direct product of N and G, i.e. $N \times G$.

c) We define $\varphi : N \rtimes_c G \longrightarrow \hat{G} = GN = NG$ (since N is normal in NG)

$(n,g) \longmapsto ng$

we prove that φ is an isomorphism.

Injectivity: Suppose $\varphi(n,g) = \varphi(n',g')$ for $(n,g), (n',g') \in N \rtimes_c G$. Then $ng = n'g'$. This implies that $n'^{-1}n = g'g^{-1}$. But $n'^{-1}n \in N \cap G$, and similarly $g'g^{-1} \in N \cap G$. Since $N \cap G = \{1\}$, we have that $n' = n$ and $g' = g$. Therefore $(n,g) = (n',g')$. This proves the injectivity.

Surjectivity: Obvious from the definition of φ.

It remains to show that φ is a homomorphism. We have

$$\begin{aligned}\varphi((n,g)(n',g')) &= \varphi(n\, c_g(n'), gg') \\ &= n\, c_g(n')\, gg' \\ &= n(g n' g^{-1}) g g' \\ &= ngn'g' \\ &= \varphi(n,g)\,\varphi(n',g').\end{aligned}$$

This proves that φ is a homomorphism. Hence, φ is an isomorphism, since φ is also a bijection.

2) We define $\varphi : \mathbb{R}^n \rtimes_c O(n,\mathbb{R}) \longrightarrow E(n)$

$(a,A) \longmapsto f_{a,A}$, where

$f_{a,A}(x) = a + Ax$.

We prove that φ is an isomorphism.

The injectivity of φ is clear, since the kernel of φ is obviously the identity map. Next we prove that φ is a homomorphism. Let $(a,A), (b,B) \in \mathbb{R}^n \rtimes_c O(n,\mathbb{R})$. Then we have $\varphi((a,A)(b,B))$

$= \varphi(a + c_A(b), AB) = f_{a+c_A(b),AB}$. On the other hand, we have $\varphi(a,A)\varphi(b,B) = f_{a,A} \circ f_{b,B}$. Then

$f_{a,A} \circ f_{b,B}(x) = f_{a,A}(b + Bx) = a + A(b+Bx) = a + Ab + ABx$
$(x \in \mathbb{R}^n)$

$= a + c_A(b) + ABx$

$= f_{a+c_A(b),AB}(x)$.

Therefore, we obtain that φ is a homomorphism.

It remains to show that φ is a surjection.

Let $M \in E(n)$. We define $T(x) = x + M(0)$. Clearly, $T \in E(n)$. Then $T(0) = M(0)$. Hence, $T^{-1}M(0) = 0$.

We denote $\tilde{M} := T^{-1}M$. We clearly have $\tilde{M} \in E(n)$. Then, $|\tilde{M}(x) - 0|^2 = |x-0|^2 = |x|^2$; i.e. $|\tilde{M}(x)|^2 = |x|^2$. for any $x \in \mathbb{R}^n$, $\tilde{M}(0)$

This implies that $x^T \tilde{M}^T M x = x^T x \quad \forall x \in \mathbb{R}^n$. Therefore, we have $\tilde{M}^T \tilde{M} = 1$, i.e. $\tilde{M} \in O(n,\mathbb{R})$.

Therefore, $\tilde{M} = T^{-1}M = \varphi(0, A)$ for some $A \in O(n, \mathbb{R})$.

Hence, $M = T\varphi(0, A) = \varphi(M(0), 1)\,\varphi(0, A)$
$= \varphi(M(0), A)$, i.e. the map φ is a surjection.

3) First we show that $D_2 = \{\pm 1\} \times_c \{\pm 1\}$ is isomorphic to V_4. We define $\varphi : D_2 \longrightarrow V_4$ via $(a, d) \longmapsto \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$. It is easy to show that φ defines an isomorphism.

Next we prove that $D_3 = \{1, \rho, \rho^2\} \times_c \{\pm 1\}$ is isomorphic to S_3. Here $\rho = e^{\frac{2\pi i}{3}}$. We define $\varphi : D_3 \longrightarrow S_3$ via $(1,1) \mapsto (1)$, $(\rho, 1) \mapsto (123)$, $(\rho, -1) \mapsto (12)$, $(\rho^2, 1) \mapsto (132)$, $(\rho^2, -1) \mapsto (13)$ and $(1, -1) \mapsto (23)$. It is easy to see that φ defines an isomorphism.

Blatt 6 - Solutions

4) Let $x := (1, 0, \dots 0) \in (\mathbb{Z}/p\mathbb{Z})^n$. The group $G := SL(n, \mathbb{Z}/p\mathbb{Z})$ acts from the left on $(\mathbb{Z}/p\mathbb{Z})^n$ via formal multiplication of matrices and vectors. The orbit of x under this action is the nonzero column vectors with entries in $\mathbb{Z}/p\mathbb{Z}$. So, it has order $p^n - 1$. The stabilizer of x has order $p^{n-1} \mid SL(n-1, \mathbb{Z}/p\mathbb{Z}) \mid$, since the elements in the stabilize of x looks like:

$$\begin{pmatrix} 1 & * & * \dots \\ 0 & & \\ 0 & & \boxed{n-1 \times n-1} \end{pmatrix}.$$

Hence, $|G| = (p^n - 1)\, p^{n-1} \mid SL(n-1, \mathbb{Z}/p\mathbb{Z}) \mid$

$$= p^{\frac{n(n-1)}{2}} \prod_{j=2}^{n} (p^j - 1), \quad \text{) by induction}$$

5) We have 4 orbits, namely the set $S_0 := \{0\}$, and the set of vectors S_{odd}, S_2 and S_4. Here S_{odd} is the set of vectors having odd number of 1's, and S_2 and S_4 are the sets of having 2, respectively 4 number of 1's.

To prove that S_* are indeed the orbits, we proceed in two ways.

Way 1: First note that every vector is in exactly one of these sets. We need to show that each of the S_* is invariant under $G := O(4, \mathbb{Z}/2\mathbb{Z})$; and that G acts transitively on S_*. For S_0 this is trivial. As an example we treat here the case S_{odd}. Note that a vector x is in S_{odd} iff $x^T x = 1$. Let $A \in G$ and $x \in S_{odd}$. Then $(Ax)^T(Ax) = x^T A^T A x = x^T x = 1$, i.e. $Ax \in S_{odd}$. This proves that S_* is invariant under G. Secondly, we show that G acts transitively on S_{odd}. Let $e = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \in S_{odd}$ and $y \in S_{odd}$, we need to find $A \in G$ s.t. $Ae = y$, i.e. $\exists A \in G$ whose first column is y. If y has only one 1, then we take for A, any permutation matrix whose first column is y. If y has 3 ones, then we take for A the matrix who has in

each column exactly one zero and whose first column equals g.

Way 2: Using SAGE we calculate the order of G:

- $S = GL(4, GF(2))$
- Ourgroup = [g for g in S if S(g.matrix().transpose()) *g == S(1)]
- len(Ourgroup)
- ...

Then we see that Permutation matrices, say P, has index 2 in G. Namely we have $G/P = \{P, gP\}$, where $g = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}$. We have obviously $P\backslash(\mathbb{Z}/2\mathbb{Z})^4 = \{S_0, S_1, S_2, S_3, S_4\}$. But we have $G\backslash(\mathbb{Z}/2\mathbb{Z})^4 = \{S_0, S_1, S_2, S_4\}$, since $gS_0 = S_0$, $gS_2 = S_2$, $gS_4 = S_4$ and $gS_1 = S_3$.