VE203 Assignment 6

Name: YIN Guoxin Student ID: 517370910043

Q1.

(i) To prove that $\star$ is a well-defined function, we need to prove that for $a, b, c, d \in G$, if $aH = cH$ and $bH = dH$, then $(aH) \star (bH) = (cH) \star (dH)$, i.e. $(a \cdot b)H = (c \cdot d)H$.

We first prove that if $H \leq G$, $h \in H$, then $hH = H$. This comes from if $x \in hH$, then $x = hh_1$ for $h_1 \in H$. Since both $h, h_1 \in H$, $x = hh_1 \in H$, which means $hH \subseteq H$. If $x \in H$, then $x = hh^{-1}x$, since $h^{-1} \in H$ due to $h \in H$ and also $x \in H$, we have $h^{-1}x \in H$. Therefore, $x \in hH$, which means $H \subseteq hH$. Therefore, if $H \leq G$, $h \in H$, then $hH = H$. This comes from if $x \in hH$, then $x = hh_1$ for $h_1 \in H$.

If H is normal, we must have for $a \in G, H \leq G, h_1, h_2 \in H$, $aH = Ha$. If $x \in aH$, then $x = ah_1 = ah_1a^{-1}a$. Since $ah_1a^{-1} \in H$, we have $x \in Ha$, which means $aH \subseteq Ha$. Similarly, if $x \in Ha$, then $x = h_2a = aa^{-1}h_2a$. Since $a \in G$, we have $a^{-1} \in G$, then $a^{-1}h_2a \in H$, we have $x \in aH$, which means $Ha \subseteq aH$. Therefore, $aH = Ha$.

Since $aH = cH$, we must have $a = ae = ch_1$ for $h_1 \in H$ and $b = be = dh_2$ for $h_2 \in H$. Then $(a \cdot b)H = (c \cdot h_1 \cdot d \cdot h_2)H = (c \cdot h_1 \cdot d)(h_2H) = (c \cdot h_1 \cdot d)H = (c \cdot h_1)Hd = c(h_1H)d = cHd = (c \cdot d)H$, which means it is a well-defined function.

- For $a, b, c \in G$, $((aH) \star (bH)) \star (cH) = ((a \cdot b)H) \star (cH) = ((a \cdot b) \cdot c)H = (a \cdot (b \cdot c))H = (aH) \star ((b \cdot c)H) = (aH) \star ((bH) \star (cH))$.
- (eH) is the identity element in X, where e is the identity element $e \in G$. It is followed from $(aH) \star (eH) = (eH) \star (aH) = (a \cdot e)H = (e \cdot a)H = aH$.
- For $a \in G$, $a^{-1} \in G$, therefore, for $aH \in X$, we can find $a^{-1}H \in X$ such that $(aH) \star (a^{-1}H) = (a^{-1}H) \star (aH) = eH$.

(ii) $D_4 = \{e, (13), (02), (01)(23), (02)(13), (03)(12), (0123), (0321)\}$ is a subgroup of S_4 but $(X, \star)$ is not a group because the $\star$ here isn't well-defined. For example, we can have $a = e_{S_4}, b = (01), c = (0123), d = (01)$, which means $aH = H = cH$, $bH = dH$. However, since $a \cdot b = (01), c \cdot d = (023)$, we have $(a \cdot b)H \neq (c \cdot d)H$, hence the $\star$ here isn't well-defined.

Q2. To begin with, the matrix multiplication is a well-defined function, which send the product of two 2×2 matrices into one 2×2 matrix.

- For all $x, y, z \in G$, suppose $x = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, $y = \left(\begin{smallmatrix} e & f \\ g & h \end{smallmatrix}\right)$, $z = \left(\begin{smallmatrix} m & n \\ p & q \end{smallmatrix}\right)$, we have

$$\begin{aligned}
x \star (y \star z) &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \star \begin{pmatrix} em + fp & en + fq \\ gm + hp & gn + hq \end{pmatrix} \\
&= \begin{pmatrix} aem + afp + bgm + bhp & aen + afq + bgn + bhq \\ cgm + chp + dgm + dhp & cgn + chq + dgn + dhq \end{pmatrix} \\
(x \star y) \star z, &= \begin{pmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{pmatrix} \star \begin{pmatrix} m & n \\ p & q \end{pmatrix} \\
&= \begin{pmatrix} aem + bgm + afp + bhp & aen + bgn + afq + bhq \\ cgm + dgm + chp + dhp & cgn + dgn + chq + dhq \end{pmatrix} \\
&= x \star (y \star z).
\end{aligned}$$

- There exists an identity, which is the identity matrix $e = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \in G$, such that for all $x = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G$, we have

$$x \star e = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \star \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \star \begin{pmatrix} a & b \\ c & d \end{pmatrix} = e \star x = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = x.$$

And for all $x = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G$, there exists $a = \left(\begin{smallmatrix} \frac{d}{ad-bc} & \frac{b}{bc-ad} \\ \frac{c}{bc-ad} & \frac{a}{ad-bc} \end{smallmatrix}\right) \in G$ such that $x \star a = a \star x = e$.

$A = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$, $A^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$ and $A^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = e$, which means the order of A is 3.

$B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $B^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, $B^3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = e$, and $B^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = e$, which means the order of B is 4.

$A \cdot B = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$, $(A \cdot B)^2 = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}$, $(A \cdot B)^3 = \begin{pmatrix} 1 & 0 \\ -3 & 1 \end{pmatrix} = e$, and we guess that $(A \cdot B)^n = \begin{pmatrix} 1 & 0 \\ -n & 1 \end{pmatrix}$. Suppose that for $k \leq 3, k \in \mathbb{N}$, we have $(A \cdot B)^k = \begin{pmatrix} 1 & 0 \\ -k & 1 \end{pmatrix}$, then $(A \cdot B)^{k+1} = \begin{pmatrix} 1 & 0 \\ -k & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -(k+1) & 1 \end{pmatrix}$. which means the order of $A \cdot B$ is infinity.

Q3. Since $\begin{pmatrix} 0&1&0&0 \\ 0&0&0&1 \\ 0&0&1&0 \\ 1&0&0&0 \end{pmatrix}^2 = \begin{pmatrix} 0&0&0&1 \\ 1&0&0&0 \\ 0&0&1&0 \\ 0&1&0&0 \end{pmatrix}$, $\begin{pmatrix} 0&1&0&0 \\ 0&0&0&1 \\ 0&0&1&0 \\ 1&0&0&0 \end{pmatrix}^3 = \begin{pmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 0&0&1&0 \\ 0&0&0&1 \end{pmatrix}$, which means $n = 3$.

Q4. Since p is prime, $p > 1$. Since $\varphi(p^k)$ is the number of $0 < m < p^k$ such that m and p^k are relatively prime. Since we know that for $a = p \times n$ such that $1 \leq n \leq p^{k-1} - 1$, we have $0 < a < p^k$ such that the common divisor of p^k and a is at least p, which means they are not relatively prime. And the number of a is simply p^{k-1} since the choice of the natural number n is from 1 to $p^{k-1} - 1$. For those numbers c such that $1 < c < p^k$ but $c \neq p \times n$, the greatest common divisor of c and p^k is 1. This is because the divisor of p^k is 1 and p^b such that $0 \leq b \leq k-1$ since p is prime, the latter of which can be interpreted as a but c cannot be one of a. Therefore, c and p^k are relatively prime. Therefore, $\varphi(p^k)$ is the total number of numbers such that $0 < m < p^k$ minus the number of a, which is

$$\varphi\left(p^k\right) = p^k - p^{k-1}.$$

Q5. Since $n^4 + 3n^2 + 1 = n(n^3 + 2n) + n^2 + 1$, $n^3 + 2n = n(n^2 + 1) + n$ and $n^2 + 1 = n \cdot n + 1$, gcd $(n^4 + 3n^2 + 1, n^3 + 2n)$ =gcd $(n^3 + 2n, n^2 + 1)$=gcd$(n^2 + 1, n)$=gcd$(n, 1)$=1. Therefore, $n^4 + 3n^2 + 1, n^3 + 2n$ and $n^3 + 2n, n^2 + 1$ are relatively prime.

Q6. Suppose a cyclic group $(\langle a \rangle, \cdot)$, where $\langle a \rangle = \{a^m | m \in \mathbb{Z}\}$, and $H \leq \langle a \rangle$. If $H = \{e\}$, it is obvious that it is a cyclic group C_1. If $H \neq \{e\}$, since $H \subseteq \langle a \rangle$, all the elements in H can be written in the form of a^p. And we denote the $\leq -$least exponential number p as k. Therefore, for any element a^n in H, by the Division Algorithm, we can write $n = mk + r$, where $0 \leq r < k$. Therefore, $a^r = a^{n-mk} = a^n \cdot a^{-mk} = a^n \cdot (a^{-m})^k$. Since $a^m \in H$, since the inverse a^{-m} of the element $a^m \in H$ must also be in H. Besides, because the group is enclosed by the group operation $\cdot$, the product of a^{-m} to the power of k also exists in H. Due to the same reason, the product of a^n and $(a^{-m})^k$ also exists in H, i.e. $a^r \in H$. But our assumption is that m is the $\leq -$least exponential number p since $r < m$. Therefore, r must be zero to make $a^r = e$. Therefore, we have $n = mk$ and $a^n = (a^k)^m$, which means all the elements in H can be written in the form of power of a^k, which means $H = \langle a^k \rangle$.

Q7. To prove the statement, we only need to show that for $a, b, c \in \mathbb{N}$, if $3 \not| ab$, then $a^2 + b^2 \neq c^2$.

If $3 \not| ab$, it means that $3 \not| a$ and $3 \not| b$, which means that $a \equiv \pm 1 \pmod 3$ and $b \equiv \pm 1 \pmod 3$. Therefore, $a^2 \equiv 1 (\text{mod } 3)$ and $b \equiv \pm 1 \pmod 3$, which means $a^2 + b^2 = c^2 \equiv 2 (\text{mod } 3)$, i.e. $c^2 = 3k + 2$ for $k \in \mathbb{N}$. However, this leads to contradiction since $3k + 2$ cannot be a perfect square.

To prove it, suppose $3k + 2 = m^2$ for $m \in \mathbb{N}$. Therefore, we have $2 = m^2 - 3k = (m + \sqrt{3k})(m - \sqrt{3k})$. Hence, $m + \sqrt{3k} = 2$ and $m - \sqrt{3k} = 1$, which means $m = \frac{3}{2}$, which is not a natural number. Therefore, we won't have $a^2 + b^2 = c^2$ for $a, b, c \in \mathbb{N}$ if $3 \not| ab$.

Q8.

Since $((\mathbb{Z}/11\mathbb{Z})^*, \otimes_{11})$ has order of 10, by Lagrange's Theorem, the only possible orders for its elements are 1,2,5 and 10.

Start with 2, $[2]_{11}^2 = [4]_{11}$, $[2]_{11}^5 = [10]_{11}$, $[2]_{11}^{10} = [1]_{11}$, therefore, $\langle [2]_{11} \rangle = ((\mathbb{Z}/11\mathbb{Z})^*, \otimes_{11})$, 2 is a generator of $((\mathbb{Z}/11\mathbb{Z})^*, \otimes_{11})$.

Q9. Suppose the inverse of $[12]_{89}$ is $[m]_{89}$. Therefore, we must have $12m \equiv 1 \pmod{89}$, which means

$12m = 89k + 1$, for $k \in \mathbb{N}$.

$$\begin{aligned}
89 &= 7 \cdot 12 + 5 \\
12 &= 2 \cdot 5 + 2 \\
5 &= 2 \cdot 2 + 1 \\
1 &= 5 - 2 \cdot 2 = 5 - 2 \cdot (12 - 2 \cdot 5) = 5 \cdot 5 - 2 \cdot 12 \\
&= 5 \cdot (89 - 7 \cdot 12) - 2 \cdot 12 \\
&= 5 \cdot 89 - 37 \cdot 12 \\
[1]_{89} &= [-37]_{89} \otimes [12]_{89} \\
[1]_{89} &= [52]_{89} \otimes [12]_{89}
\end{aligned}$$

Through calculation, I find that when m=52, we have $12 \times 52 = 624 = 89 \times 7 + 1$. Therefore, the inverse of $[12]_{89}$ is $[52]_{89}$.

Q10. Since $2|56, 7|56$,

$$\varphi(56) = 56 \cdot (1 - \frac{1}{2})(1 - \frac{1}{7}) = 24$$

Therefore the order of $((\mathbb{Z}/56\mathbb{Z})^*, \otimes 56)$ is 24. By Lagrange Theorem, the order of $[27]_{56}$ is 1,2,3,4,6,8,12,24. Now, $27^2 = 729$, since $729 \equiv 1 \pmod{56}$, therefore, the order of it is 2.

Q11. The Cayley Table of $((\mathbb{Z}/9\mathbb{Z})^*, \otimes_9)$ is

$\otimes_9$	$[1]_9$	$[2]_9$	$[4]_9$	$[5]_9$	$[7]_9$	$[8]_9$
$[1]_9$	$[1]_9$	$[2]_9$	$[4]_9$	$[5]_9$	$[7]_9$	$[8]_9$
$[2]_9$	$[2]_9$	$[4]_9$	$[8]_9$	$[1]_9$	$[5]_9$	$[7]_9$
$[4]_9$	$[4]_9$	$[8]_9$	$[7]_9$	$[2]_9$	$[1]_9$	$[5]_9$
$[5]_9$	$[5]_9$	$[1]_9$	$[2]_9$	$[7]_9$	$[8]_9$	$[4]_9$
$[7]_9$	$[7]_9$	$[5]_9$	$[1]_9$	$[8]_9$	$[4]_9$	$[2]_9$
$[8]_9$	$[8]_9$	$[7]_9$	$[5]_9$	$[4]_9$	$[2]_9$	$[1]_9$

Yes, it is cyclic. Since it is a group with order 6, the possible order of its elements are 1,2,3,6. For the element $[2]_9$ in it, we can see that $([2]_9)^2 = [4]_9, ([2]_9)^3 = [8]_9$, which means the order of it must be greater than 3. Therefore, the only choice of this element is 6, which means the group is cyclic.

Q12.

(i) Denote the $\gcd(s, n) = g$, then $s = cg$ and $n = mg$ for $c \in \mathbb{N}$ and $\gcd(c, m)$=1, then we have,

$$a^{sm} = a^{s \frac{n}{\gcd(s,n)}} = a^{cn} = (a^n)^b = e^c = e.$$

Suppose $0 < p \leq n$ such that $a^{sp} = e$ and p is the $\leq -$least such thing, i.e. the order of b is p. Then $p|n = p|(mg)$ by Lagrange Theorem and $n|sp$ since the order of a is n. Rewrite $n|sp$ into $mg|(cg \cdot p)$. Factor out g and we have $m|cp$. Since $\gcd(c, m) = 1$, we have $m|p$, which means $m \leq p$. Since p is the $\leq -$least such thing, we must have $m = p$.

(ii) Denote $\langle a^t \rangle_G$ as C_x and$\langle b \rangle_G$ as C_m.

- If $\langle a^t \rangle_G = \langle b \rangle_G$, the order of these two groups must be the same, which means

$$m = \frac{n}{\gcd(s, n)} = x = \frac{n}{\gcd(t, n)},$$

which means $\gcd(s, n) = \gcd(t, n)$.

- If $\gcd(s, n) = \gcd(t, n)$, then $x = m$, i.e. the order of this two groups are the same. We will prove that $\langle a^t \rangle_G = \langle a^g \rangle_G = \langle a^s \rangle_G$, where $g = \gcd(s, n) = \gcd(t, n)$.

  For every element a^{us} in $\langle a^s \rangle_G$, since $s = cg$, we know that $a^{us} = a^{ucg} = (a^g)^{uc}$, which means it must be an element in $\langle a^g \rangle_G$. For each element $a^w g$ in $\langle a^g \rangle_G$, by BéZout's Lemma, $g = xs + yn$, then $a^w g = a^{w(xs+yn)} = a^{wxs} a^{wyn} = (a^s)^{wy} (a^n)^{wy} = (a^s)^{wy}$, which means it must be an element in $\langle a^g \rangle_G$. Therefore, $\langle a^g \rangle_G = \langle a^s \rangle_G$. Similarly, we can prove that $\langle a^g \rangle_G = \langle a^t \rangle_G$. Therefore, $\langle a^t \rangle_G = \langle a^s \rangle_G$, i.e. $\langle a^t \rangle_G = \langle b \rangle_G$.