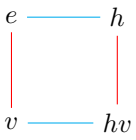
MATH 410 Homework 3

Qilin Ye

February 22, 2021

2.2.1 See the diagram below, where the red lines refer to multiplying by v and cyan lines refer to multiplying by h.



2.2.9 & 2.2.10 See the matrices below.

$$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \qquad \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

The main difference is that the one for 2.2.9 has two 1's each row (and column) since the generating set contains two elements, whereas the one for 2.2.10 has three 1's due to the three elements F, R, R^{-1}.

2.3.3 $\mathbb{Z}/6\mathbb{Z}^\times = \{1,5\}, \mathbb{Z}/8\mathbb{Z}^\times = \{1,3,5,7\}$, and $\mathbb{Z}/12\mathbb{Z}^\times = \{1,5,7,11\}$. For the second part, notice that all positive integers not exceeding p^e that are coprime to p^e are multiples of p since that's the only prime divisor of p^e. There are p^{e-1} such numbers, so taking them away gives $\varphi(p^e) = p^e - p^{e-1}$.

2.3.5 The determinant of this inverse is $[1][4] - [2][3] = [5]$ whose inverse is $[3]$ since $[5][3] = [1]$. Therefore,

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}^{-1} = [3] \begin{bmatrix} [4] & [-2] \\ [-3] & [1] \end{bmatrix} = \begin{bmatrix} 5 & 1 \\ 5 & 3 \end{bmatrix}.$$

Applying the formula (choosing first row and then second which needs to be linearly independent form the first), we have $|\mathrm{GL}(2, \mathbb{Z}/7\mathbb{Z})| = (49-1)\cdot(49-7) = 2016$.

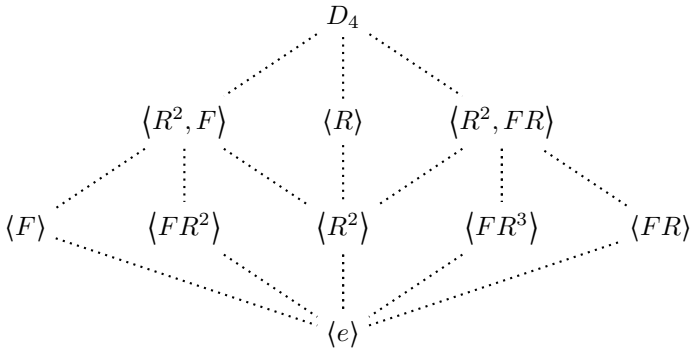
2.4.8 By Lagrange, since $|D_4| = 8$, possible orders of subgroups include $1, 2, 4$, and 8, and so proper subgroups can either contain 2 or 4 elements.

(1) Trivial subgroups: $\{I\}$ and D_4.

(2) Proper subgroups with order 2: subgroups generated by one element of order 2: $\langle F \rangle, \langle FR^2 \rangle, \langle R^2 \rangle, \langle FR^3 \rangle$, and $\langle FR \rangle$.

(3) Proper subgroups with order 4: either generated by one element of order 4, i.e.,$\langle R\rangle$, or generated by two elements, both of order 2: $\langle R^2, F\rangle = \{I, R^2, F, FR^2\}$ or $\langle R^2, FR^2\rangle = \{I, R^2, FR, FR^3\}$.

The poset diagram is below:



2.4.10 Take any $a, b \in Z(G)$. We want to show that $ab^{-1} \in Z(G)$ (commutativity is trivial in this context). Indeed, for any $x \in G$ we have

$$ab^{-1}x = a(b^{-1}x) = a(xb^{-1}) = (ax)b^{-1} = xab^{-1},$$

and the claim follows.

2.4.12 Suppose our center's first row is of form $[a, b]$. Let $A = \begin{bmatrix} x & y \\ 0 & 1 \end{bmatrix}$ be any element of the affine group. Then

$$\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}\begin{bmatrix} x & y \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} ax & ay+b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} x & y \\ 0 & 1 \end{bmatrix}\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} ax & bx+y \\ 0 & 0 \end{bmatrix},$$

from which we obtain the necessary and sufficient condition $ay + b = bx + y$, independent of choice of (x, y). Letting $x = y = 1$, we have $a + b = b + 1$ and so $a = 1$. Now the original equation reduces to $y + b = bx + y$ and so $b = bx$ for all b. Now take $x = 2$. Then $b = 2b$ and so $b \equiv 2b \pmod p \implies b \equiv 0 \pmod p$ and so $b = 0$. Hence the affine group has a trivial center.

2.5.3 $o(a^k)$ denotes the smallest positive integer p such that $(a^k)^p$ becomes the identity. Note that the identity here is of form $(a^n)^m$ for some positive integer m, i.e., powers of itself. Therefore, for some $m \in \mathbb{N}$ we have

$$(a^k)^p = a^{kp} = (a^n)^m = a^{mn}.$$

Therefore this question reduces to finding the smallest p such that $n \mid kp$. Therefore for any common divisor d of n and k, one has $(n/d) \mid (kp)/d$. Letting $d := \gcd(n, k)$ gives

$$\frac{n}{\gcd(n,k)} \,\Big|\, \frac{k}{\gcd(n,k)}p.$$

Note that $n/\gcd(n, k)$ is coprime to $k/\gcd(n, k)$ (otherwise we can divide both sides by some nontrivial factor, and $\gcd(n, k)$ times this factor gives us an even larger gcd, contradiction). Therefore by Euclid's lemma

$$\frac{n}{\gcd(n,k)} \,\Big|\, p$$

and so the smallest p is $n/\gcd(n, k)$ itself. Indeed,

$$(a^k)^{n/\gcd(n,k)} = a^{kn/\gcd(n,k)} = (a^n)^{k/\gcd(n,k)} = e^{k/\gcd(n,k)} = e.$$