1.6.6b) If $a,b,c,d \in \mathbb{Z}$, $n \in \mathbb{Z}^+$ show that

$a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ imply that

$ac \equiv bd \pmod{n}$

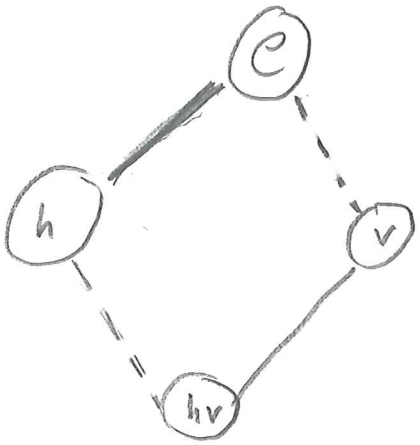
We know $a = b + in$ and $c = d + jn$ for $i,j \in \mathbb{Z}$

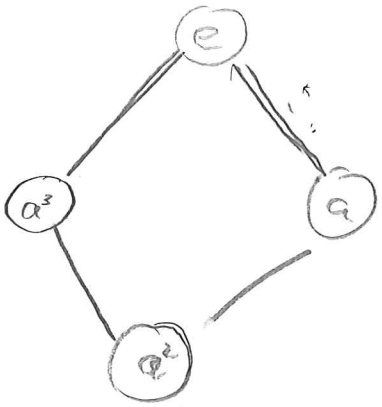
Furthermore $(b+in)(d+jn) = bd + ind + bjn + ijn^2$

So $ac = bd + ind + bjn + ijn \equiv bd \pmod{n}$

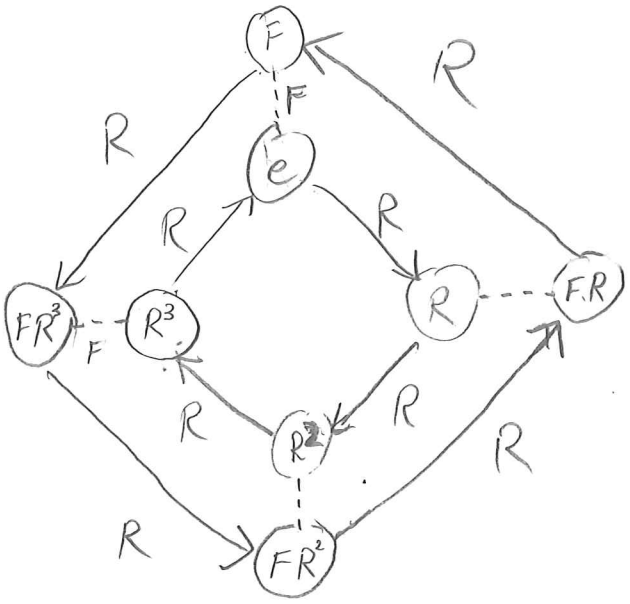
2.2.1. Draw a Cayley graph for the Klein 4-group $\mathbb{Z}_2^2$ with generating set $\{h, v\}$ for $h=(1,0)$ $v=(0,1)$

Compare with the Cayley graph of C_4 with generating set $\{a, a^{-1}\}$





2.2.5 Draw a Cayley graph for D_4 with generating set $\{R, F\}$



2.3.3a) Prove that

$$\phi(6) = 2 \quad \phi(8) = 4 \quad \phi(12) = 4$$

by listing all elements of $\mathbb{Z}_n^*$ for $n = 6, 8, 12$

$$\mathbb{Z}_6^* = \{1, 5\}$$

$$\mathbb{Z}_8^* = \{1, 3, 5, 7\}$$

$$\mathbb{Z}_{12} = \{1, 5, 7, 11\}$$

b) Show that $\phi(p^e) = p^e - p^{e-1}$ for any prime p, exponent $e = 1, 2, \ldots$

$$\phi(p^e) = p^e - 1 - \left(\begin{array}{l}\text{number of integers } q \text{ such that } 1 \leq q \leq p^e \\ \text{and } \gcd(p, q) > 1\end{array}\right)$$

Since p is prime $\gcd(p, q) > 1$ if and only if q is a multiple of p. So q is of the form kp for $1 \leq k < p^{e-1}$

There are $p^{e-1} - 1$ such numbers, so $\phi(p^e) = p^e - 1 - (p^{e-1} - 1)$

$$= p^e - p^{e-1}$$

2.3.8 Which of the following groups are commutative

Assume $n \in \mathbb{Z}$ and $n \geq 2$

a) $\mathbb{Z}_n^{2\times 2}$, the group of 2×2 matrices with entries in $\mathbb{Z}_n$ under addition

Yes, since $\mathbb{Z}_n$ is commutative

b) The group of proper rotations of a cube

No, two rotations around different axes do not commute

2.3.8 c) $\mathbb{Z}_n^2$, the group of 2-vectors with entries in $\mathbb{Z}_n$ under addition

Yes, since $\mathbb{Z}_n$ is commutative

d) $\mathbb{Z}_n^{2\times 2}$, the 2×2 matrices g with entries in $\mathbb{Z}_n$ s.t. $\det(g) \in \mathbb{Z}_n^*$, under matrix multiplication

No. Consider the following matrices

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$$

These two products are not equal, since $2 \neq 1$ in $\mathbb{Z}_n$ for $n \geq 2$

2.4.2 Find all the powers of 2 in $\mathbb{Z}_{11}^*$ and $\mathbb{Z}_{13}^*$.

in $\mathbb{Z}_{11}^*$: $2^0 = 1$ $2^1 = 2$ $2^2 = 4$ $2^3 = 8$

$2^4 = 5$ $2^5 = 10$ $2^6 = 9$ $2^7 = 7$

$2^8 = 3$ $2^9 = 6$ $2^{10} = 1$

in $\mathbb{Z}_{13}^*$: $2^0 = 1$ $2^1 = 2$ $2^2 = 4$ $2^3 = 8$

$2^4 = 3$ $2^5 = 6$ $2^6 = 12$ $2^7 = 11$

$2^8 = 9$ $2^9 = 5$ $2^{10} = 10$ $2^{11} = 7$

$2^{12} = 1$

2.4.4 Find the order of all elements of the unit group $\mathbb{Z}_{11}^*$. Then do the same for the unit group $\mathbb{Z}_{13}^*$

$\mathbb{Z}_{11}^*$: $1^1 = 1$, so order 1

$2^{10} = 1$ so order 10

$3^5 = 1$ so order 5

$4^5 = 1$ so order 5, since $4 = 2^2$

$5^5 = 1$ so order 5

$6^{10} = 1$ so order 10 Check $6^2 \equiv 3 \pmod{11}$ $6^5 \equiv 10 \pmod{11}$

$7^{10} = 1$ so order 10

$8^{10} = 1$ so order 10

$9^5 = 1$ so order 5

$10^2 = 1$ so order 2

Trick: Only need to check a^1, a^2, a^5, a^{10}

since any subgroup of $\mathbb{Z}_{11}^*$ has order divisible by the order of $\mathbb{Z}_{11}^*$, which is 10

2.4.4. $\mathbb{Z}_{13}^*$ Order of $\mathbb{Z}_{13}^*$ is 12, so need to check a^1, a^2, a^3, a^4, a^6

$1^1 = 1$ $\quad 4^6 = 1$ $\quad 7^{12} = 1$ $\quad 10^6 = 1$

$2^{12} = 1$ $\quad 5^4 = 1$ $\quad 8^4 = 1$ $\quad 11^{12} = 1$

$3^3 = 1$ $\quad 6^{12} = 1$ $\quad 9^3 = 1$ $\quad 12^2 = 1$

2.4.5 a) Are there any other proper subgroups of D_3 other than the ones listed in (2.8) (on p. 67)

No! Let H be a subgroup of D_3.

Assume $F \in H$, Then either $H = H_1 = \{I, F\}$ or

H contains one of the elements R, R^2, FR, FR^2

If $H \ni R$, then $H = D_3$, since F, R generate D_3

If $H \ni R^2$, then $H \ni (R^2)^2 = R$, so $H = D_3$

If $H \ni FR$, then $H \ni FFR = R$ — " —

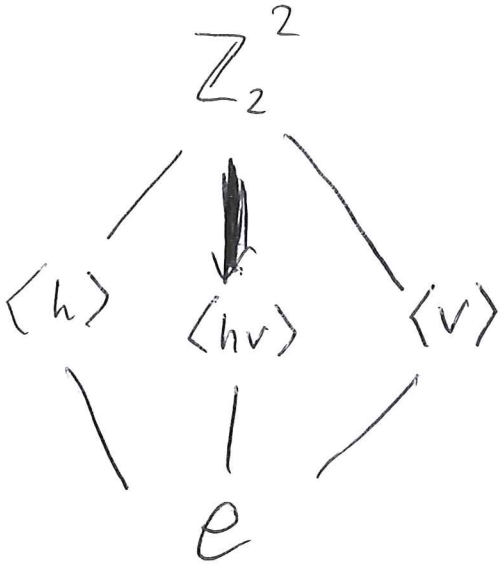
If $H \ni FR^2$, then $H \ni FFR^2 = R^2$ — " —

} here we use that H must be closed under multiplication

If $R \ni H$, then $R^2 \ni H$. If H is different from $H_4 = \{1, R, R^2\}$, then H must contain F, FR, FR^2, but then $H = D_3$ since H will contain F.

Continuing these arguments show that D_3 has no other proper subgroups

2. 4.5b) Draw the poset diagram of the Klein 4-group $\mathbb{Z}_2^2$, generated by h, v



2.4.7. Draw the poset diagram for the subgroups of $\mathbb{Z}_{12}^*$ under multiplication

$$\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$$

Multiplication $5^2 = 1$ $7^2 = 1$ $11^2 = 1$

$5 \cdot 7 = 11$ $5 \cdot 11 = 7$

$7 \cdot 11 = 5$

This group is isomorphic to $\mathbb{Z}_2^2$, so

Same poset diagram as previous exercise