

Exercise 4.66: Note that $U(2^n)$ is the set of all odd naturals (relatively prime to 2^n) less than 2^n . Note that $U(2^n) \subseteq U(2^{n+1})$. Note that $U(2^3) = U(8)$ is non cyclic, this is left as an exercise to the reader and is simply a bit of brute force.

Suppose $U(2^n)$ is non-cyclic.

Suppose $U(2^{n+1})$ is cyclic.

There exists an element call it a that is a generator of $U(2^{n+1})$. Define a' using the division algorithm (dividing a by 2^n) $a = j2^n + a'$. Note that $a' = a - j2^n$ and that since $j2^n$ is even and a is odd a' must be odd and thus an element of $U(2^n)$. Choose $x \in U(2^n)$. Note that $x \in U(2^{n+1})$, thus there exists a natural k such that $a^k \bmod 2^{n+1} = x$. Note that we could write $x = a^k - i2^{n+1} = (j2^n + a')^k - i2^{n+1} = j^k(2^n)^k + 2a'j2^n + a'^k - i2^{n+1} = a'^k - (2i - j^k(2^n)^{k-1} - 2a'j)2^n$ thus $a'^k \bmod 2^n = x$. Noting that a' is a generator for $U(2^n)$ we conclude that $U(2^n)$ is cyclic, a contradiction, thus $U(2^{n+1})$ is non cyclic.

By induction $U(2^n)$ is non cyclic for all $n \geq 3$.

Exercise 4.72: For each of these it would simply be the greatest common divisor between 48 and the power of a .

1. $\langle a^3 \rangle$
2. $\langle a^{24} \rangle$
3. $\langle a^6 \rangle$

Exercise 4.74: Note that all elements of H have determinant of 1 and thus $H \subseteq GL(2, \mathbb{R})$.

Note that $a = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in H$. Also note that its inverse $a^{-1} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \in H$. Note that a

increments the upper right hand value of a matrix in H , $a \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & n+1 \\ 0 & 1 \end{bmatrix}$, thus a along with a^{-1} can generate all elements in H . Noting that the identity is in H we can conclude H is a cyclic sub group of $GL(2, \mathbb{R})$.

Exercise 4.81: For all cases there is the set of all rotations, a cyclic sub group of order n . If n is odd there are no other sub groups of order n . If n is even we can inscribe it (see attached) inside of two $D_{n/2}$ and their set of operations will give us two additional sub groups of order n . Thus if n is odd there is one sub group of order n and if n is even there are three sub groups of order n .

Exercise 4.82: Note that G is clearly closed as the addition of two integers mod 3 will be in $\{0, 1, 2\}$. Also note that there is an identity namely 0. The inverse is trivial $a_1x^2 + a_2x + a_3$ has an inverse of $b_1x^2 + b_2x + b_3$ where b_k is the inverse of a_k in \mathbb{Z}_3 . Also addition is associative and thus we know this is a group. By simply observing permutations we can see that there are 3 possibilities for each coefficient, thus $|G| = 3 * 3 * 3 = 27$. Suppose $a_1x^2 + a_2x + a_3$ is a generator for G . Note that $a_k \neq 0$, since if a a_k were 0 we would never obtain the elements where that coefficient was non-zero ie $0x^2 + a_2x + a_3$ can never generate x^2 which

is in G . We can now conclude that two of our coefficients are the same since there are three coefficients and two possibilities (pigeonhole principal), without loss of generality assume these are a_1 and a_2 . Since $a_1x^2 + a_2x + a_3$ is a generator we know that there exists a k such that $(a_1x^2 + a_2x + a_3)^k = x^2$, however since $a_1 = a_2$ we know that those two coefficients will always be the same and thus the first coefficient being one implies that the second coefficient will be one, in other words no such k could exist. We conclude the negation of our supposition and conclude that G has no generator and thus is non cyclic.

Exercise 4.83: Note that if m and n are relatively prime the only shared element between $\langle a \rangle$ and $\langle b \rangle$ will be the identity, since any shared element must have a order that divides both m and n . Thus $a^k = b^k$ implies that $a^k = b^k = e$. Note that $m \mid k$ and $n \mid k$, thus $\text{gcm}(m, n) \mid k$. Note that $\text{gcm}(m, n) = mn$ and thus $mn \mid k$.