Assignment 2 Solutions

24. Let p and q be distinct primes. How many generators does $\mathbb{Z}_{pq}$ have?

$\mathbb{Z}_{pq}$ has $pq - p - q + 1$ generators.

By Cor. 4.14 we know that the generators of $\mathbb{Z}_{pq}$ are the integers r s.t. $1 \le r < pq$ and $\gcd(r, pq) = 1$

To count these note that since p, q are prime then if $\gcd(r, pq) > 1 \Rightarrow p \mid n$ or $q \mid n$ (or both)

The integers r, $1 \le r < pq$ where $p \mid r$ are $p, 2p, \ldots, (q-1)p$,

the integers r, $1 \le r < pq$ where $q \mid r$ are $q, 2q, \ldots, (p-1)q$ and

$\therefore$ there are $(p-1) + (q-1)$ integers in $1, \ldots, pq$ not relitivly prime to pq

$\therefore$ $\mathbb{Z}_{pq}$ has $(pq-1) - (p-1) - (q-1) = pq - p - q + 1$ generators

39. Prove that if G is a cyclic group of order m and $d \mid m$, then G must have a subgroup of order d.

Proof: Since G is cyclic $\Rightarrow$ $G = \langle a \rangle$ for some $a \in G$.

and $|a| = |G| = m$. If $d \mid m \Rightarrow k = \frac{m}{d}$ is an integer.

Consider $b = a^{\frac{m}{d}}$ $\quad b^d = a^{\frac{m}{d} \cdot d} = a^m = e$

$\therefore$ $|b| \le d$, but if $j < d \Rightarrow mj < md$

$b^j = a^{\frac{m \cdot j}{d}}$ and $\frac{m \cdot j}{d} < m$

$\therefore$ $a^{\frac{mj}{d}} \neq e$ since m is the smallest integer power of a which gives e. , $\therefore$ $|b| \ge d$ $\therefore$ $|b| = d$

and $H = \langle b \rangle$ is a subgroup of G with $|H| = d$. ∎

13. Let $\sigma = \sigma_1 \cdots \sigma_m \in S_n$ be the product of disjoint cycles. Prove that the order of σ is the least common multiple of the lengths of the cycles $\sigma_1, \ldots, \sigma_m$.

Proof: Let l_i = length of σ_i, by definition the order of a cycle is given by its length.

$\therefore$ $|\sigma_i| = l_i$

Let $L = \operatorname{lcm}(l_1, \ldots, l_m)$.

Disjoint cycles commute, $\therefore$

$$(\sigma)^L = (\sigma_1 \cdots \sigma_m)^L = \sigma_1^L \cdots \sigma_m^L$$

σ_i^L = identity since L is a multiple of l_i, i.e.

$$\sigma_i^L = \left(\sigma_i^{l_i}\right)^k = (id)^k = id \quad (\text{for some } k).$$

$\therefore$ $\sigma^L = id$. if we take σ^j for $j < L$

$\Rightarrow$ Exists i s.t. j is not a multiple of l_i

$\Rightarrow \sigma_i^j \neq id \Rightarrow \sigma \neq id$

$\therefore$ $|\sigma| = L = \operatorname{lcm}(l_1, \ldots, l_m)$ ∎