Abstract Algebra: Homework 4

Huize Shi - A92122910

February 8, 2018

Section 6

22.

Subgroup diagram of $\mathbb{Z}_{12}$

$$\begin{tikzcd}
 & & \mathbb{Z}_{12} \arrow[dl, dash] \arrow[dr, dash] & \\
 & \langle 2\rangle \arrow[dl, dash] \arrow[dr, dash] & & \langle 3\rangle \arrow[dl, dash] \\
\langle 4\rangle \arrow[dr, dash] & & \langle 6\rangle \arrow[dl, dash] & \\
 & \{0\} & &
\end{tikzcd}$$

23.

Subgroup diagram of $\mathbb{Z}_{36}$

$$\begin{tikzcd}
 & & \mathbb{Z}_{36} \arrow[dl, dash] \arrow[dr, dash] & & \\
 & \langle 2\rangle \arrow[dl, dash] \arrow[dr, dash] & & \langle 9\rangle \arrow[dr, dash] & \\
\langle 4\rangle \arrow[dr, dash] & & \langle 6\rangle \arrow[dl, dash] \arrow[rr, dash] & & \langle 18\rangle \arrow[ddll, dash] \\
 & \langle 12\rangle \arrow[dr, dash] & & & \\
 & & \{0\} & &
\end{tikzcd}$$

24.

Subgroup diagram of $\mathbb{Z}_8$

$$\begin{tikzcd}
\mathbb{Z}_8 \arrow[d, dash] \\
\langle 2 \rangle \arrow[d, dash] \\
\langle 4 \rangle \arrow[d, dash] \\
\{0\}
\end{tikzcd}$$

26.

$$< 0 >: \ \frac{8}{gcd(0,8)} = 1$$

$$< 1 >: \ \frac{8}{gcd(1,8)} = 8$$

$$< 2 >: \ \frac{8}{gcd(2,8)} = 4$$

$$< 3 > = < 1 >: \ \frac{8}{gcd(3,8)} = 8$$

$$< 4 >: \ \frac{8}{gcd(4,8)} = 2$$

$$< 5 > = < 1 >: \ \frac{8}{gcd(5,8)} = 8$$

$$< 6 > = < 2 >: \ \frac{8}{gcd(6,8)} = 4$$

$$< 7 > = < 1 >: \ \frac{8}{gcd(7,8)} = 8$$

All subgroups of $\mathbb{Z}_8$: $< 0 >$, $< 1 >$, $< 2 >$, $< 4 >$

29.

All subgroups of $\mathbb{Z}_{17}$: $< 0 >$, $< 1 >$. 17 is prime therefore all number from 1 to 16 are prime to 17. This means the only subgroups are $< 0 >$ and $< 1 >$

45.

Proof. Let r and s be positive integers. Show that $\{nr + ms \mid n, m \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$

Closure:

$$\begin{aligned}&(n_1r+m_1s)+(n_2r+m_2s)\\=&n_1r+n_2r+m_1s+m_2s\\=&(n_1+n_2)r+(m_1+m_2)s\end{aligned}$$

Hence show the set is closed under addition.

Identity:

$$(0r+0s)=0$$

Hence shown 0 is in the set.

Inverse: $\forall\{nr+ms \mid n,m\in\mathbb{Z}\}$, let the inverse be defined as $\{(-n)r+(-m)s \mid n,m\in\mathbb{Z}\}$.

$$\begin{aligned}&(nr+ms)+((-n)r+(-m)s)\\=&nr-nr+ms-ms\\=&0\end{aligned}$$

Hence shown that $\{nr+ms \mid n,m\in\mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$. □

50.

Proof. Since a is of order 2, $a^2=a*a=e$. Consider the following:

$$\begin{aligned}&(xax^{-1})^2\\=&(xax^{-1})(xax^{-1})\\=&xa(x^{-1}x)ax^{-1}\\=&x((ae)a)x^{-1}\\=&xx^{-1}\\=&e\end{aligned}$$

It is evident that $xax^{-1}\neq e$ because it would imply that $a=e$ which is of order 1. Since a is the unique element that has order 2, and $(xax^{-1})^2=e$, this imply that $xax^{-1}=a$, because no other element when raised to the second power would evaluates to e. Therefore the following holds:

$$\begin{aligned}xax^{-1}&=a\\xa(x^{-1}x)&=ax\\xae&=ax\\xa&=ax\end{aligned}$$

□

51.

Generators of $\mathbb{Z}_{pq}$ are defined as integers that are less than pq and are relatively prime to pq. Since there are $(p-1)$ number of multiples of q, and $(q-1)$ number of multiples of p, there are $(pq-1)-(p-1)-(q-1)$ number of integers that are less than pq and relatively prime to pq.

$$\begin{aligned}&(pq-1)-(p-1)-(q-1)\\=&pq-1-p+1-q+1\\=&pq-p-q+1\\=&(p-1)(q-1)\end{aligned}$$

There are $(p-1)(q-1)$ number of positive integers that generates $\mathbb{Z}_{pq}$.

52.

Let p be a prime number and r an integer ≥ 1. There are $p^{r-1}-1$ factors of p^r. There are p^r-1 number s less than p^r. The number of coprime integers less than p^r is as follows:

$$\begin{aligned} &(p^r-1)-(p^{r-1}-1) \\ =&p^r-1-p^{r-1}+1 \\ =&p^r-p^{r-1} \\ =&p^{r-1}(p-1) \end{aligned}$$

There are $p^{r-1}(p-1)$ number of generators of the cyclic group $\mathbb{Z}_{p^r}$ where p is a prime number and r is an integer ≥ 1.

55.

Proof. Cyclic group $C \leq G$ is the smallest possible subgroups. This means that if there exist a nontrivial proper subgroup, it must be a cyclic group of G. Given $\mathbb{Z}_p$ where p is a prime number. All $p-1$ numbers less than p are coprime to p. this means that all $p-1$ generators generates G which means that there are no proper nontrivial subgroup of $\mathbb{Z}_p$ if p is a prime number. ☐

56.

a. Let $H =< a >$ and $K =< b >$. Since $|H| = r$ and $|k| = s$, we know that because G is abelian $(ab)^{rs} = (a^r)^s(b^s)^r = e$. Guessing that $< ab >$ generates the cyclic subgroup of order rs.

Identity:

$$\begin{aligned} (ab)^n &= e \\ a^n b^n &= e \\ a^n &= b^{-n} = c \end{aligned}$$

Since c is in H and K, it generates subgroup of H with some order that divides r, and also generates subgroup of K with some order that divides s. However, since r and s are coprimes, the following is implied:

$$(| < c > | = 1) \Rightarrow (< c >= e) \Rightarrow (c = e)$$

Hence we know $a^n = b^{-n} = e$, this means that since $a^n \in H$ and $b^n \in K$, this means n must be divisible by both r and s. Hence we know $n = rs$. This means that $< ab >$ is the subgroup of order rs.

b. Let $m = gcd(r, s)$, $n = mp$ and p is prime to r and that $rp = rs/m$ is the LCM(r, s). This means that $| < a > | = r \wedge | < b^m > | = p$. Since r and q are coprimes, by part a, we know that ab^d generates the cyclic subgroup of order the LCM of r and s.