Seminar 5

Remember: If $x^n = 1$ or $nx = 0$ (depending on the operation), then $ord(x) = n$. Also, the order of the identity element is 1.

1. For $\mathbb{Z}_8$ we compute the order of an element $\hat{x}$ as the smallest $k \in \mathbb{N}^*$ such that $k \cdot \hat{x} = \hat{0}$.

   For U_6 we compute the order of an element ϵ as the smallest $k \in \mathbb{N}^*$ such that $\epsilon^k = 1$.

2. For $(K, \cdot)$ we have $\forall x \in K \setminus \{e\}$, $ord(x) = 2$. The order of the elements of $(S_3, \circ)$ are 1, 2 or 3.

   We have $(Q, \cdot) = \{\pm 1, \pm i, \pm j, \pm k\}$, hence $ord(1) = 1$, $ord(-1) = 2$ and $\forall x \in Q \setminus \{\pm 1\}, ord(x) = 4$.

   They are not cyclic, as there is no element whose order is equal to the order of the group.

3. (i) By computing matrix multiplications, we easily get: $ord(A) = 4$, $ord(B) = 2$, $ord(A \cdot B) = \infty$, $ord(B \cdot A) = \infty$.

   (ii) Take $(\mathbb{C}^*, \cdot)$ group, with $ord(2) = \infty, ord(\frac{1}{2}) = \infty$, but $ord(2 \cdot \frac{1}{2}) = ord(1) = 1 < \infty$.

4. Let $a = [m, n]$ and $d = (m, n)$. If $m = m'd$ and $n = n'd$, then $a = m'n'd = mn' = m'n$.

   (i) From $(xy)^a = x^a \cdot y^a = (x^m)^{n'} \cdot (y^n)^{m'} = 1$, so $ord(xy)$ is finite and divides a.

   (ii) If $ord(xy) = b$, then $x^b \cdot y^b = (xy)^b = 1$, so $x^b = y^{-b}$. But $x^b \in < x >$ and $y^{-b} \in < y > \Rightarrow x^b = y^{-b} = 1$. As $ord(x) = m$ and $ord(y) = n$ and $m \mid b$, $n \mid b$, so $a \mid b$, together with (i) we get $ord(xy) = [m, n]$.

   (iii) From Lagrange's theorem we have $|< x > \cap < y >|$ divides $|< x >| = m$ and $|< y >| = n$. As $(m, n) = 1$, we have $|< x > \cap < y >| = 1$. So $< x > \cap < y > = \{1\}$. So, together with (ii) we get that $ord(xy) = [m, n] = mn$.

5. Suppose $ord(xy) = m < \infty$. Then $(xy)^m = 1 \iff xy \cdot xy \dots xy = 1$ (m times) $\iff x \cdot (yx)^{m-1} \cdot y = 1$.

   If we multiply on the left by y and on the right by y^{-1}, then we get: $(yx)^m = 1$.

   This means that $ord(yx) < \infty$ and $ord(yx) \mid m$.

   Doing the same for $ord(yx) = n \Rightarrow ord(xy) < \infty$ and $ord(xy) \mid n$.

   In the end $ord(xy) = ord(yx)$.

   Also, if we take $ord(xy) = \infty$ and suppose $ord(yx) < \infty$. With the same method we'll have $ord(xy) < \infty$, which is a contradiction.

6. (i) To check if $t(G)$ is a subgroup of G, we need to check:
      i. $t(G) \neq \emptyset$
      ii. $\forall x, y \in t(G)$, i.e. $ord(x), ord(y) < \infty \Rightarrow x \cdot y \in t(G)$, i.e. $ord(xy) < \infty$.
      iii. $\forall x \in t(G) \Rightarrow x^{-1} \in t(G)$, i.e. $ord(x^{-1}) < \infty$.

      Remember that if G is abelian, $(xy)^m = x^m \cdot y^m$.

   (ii) If G is not abelian, the property is not true. (See exercise 4)

7. If $(G, \cdot) \simeq (G', \cdot) \Rightarrow \exists f : G \to G'$ group isomorphism.

   Take $g : t(G) \to t(G')$ with $g(x) = f(x)$. Then g is a group homomorphism and it is injective.

   We need to prove that g is surjective.

   Let $y \in t(G') \subseteq G'$, say $ord(y) = n$. Then $\exists x \in G$ such that $y = f(x)$ as f is bijective. Then $y^n = 1 \iff f(x)^n = 1 \iff f(x^n) = f(1) \iff x^n = 1$. Hence $ord(x) = ord(y) = m$, and so $x \in t(G)$. Hence g is surjective.

8. (i)

   $$t(\mathbb{Q}, +) = \{x \in \mathbb{Q} \mid ord(x) < \infty\} = \{0\}$$

   $$t(\mathbb{Q}^*, \cdot) = \{x \in \mathbb{Q}^* \mid ord(x) < \infty\} = \{-1, 1\}$$

   But $t(\mathbb{Q}, +) \not\simeq t(\mathbb{Q}^*, \cdot) \Rightarrow (\mathbb{Q}, +) \not\simeq (\mathbb{Q}^*, \cdot)$.

   (ii) As above.

9. (i) Let $ord(x) = n \in \mathbb{N}^*$. Then $x^n = 1$.
   As f is a group homomorphism, $[f(x)]^n = f(x^n) = f(1) = 1' \Rightarrow ord(f(x)) < \infty$ and $ord(f(x)) \mid n \iff ord(f(x)) \mid ord(x)$.

   (ii) Using (i), we consider f to be injective. Let $ord(f(x)) = m \Rightarrow f(x^m) = [f(x)]^m = 1' = f(1) \Rightarrow x^m = 1$, but $ord(x) = n \Rightarrow n \mid m$.
   We know from (i) that $ord(f(x)) \mid ord(x)$.
   Hence, $n = m \iff ord(x) = ord(f(x))$.

10. We have

$$\mathbb{Z}_4 = \{\hat{0}, \hat{1}, \hat{2}, \hat{3}\},$$
$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(\overline{0}, \overline{0}), (\overline{0}, \overline{1}), (\overline{1}, \overline{0}), (\overline{1}, \overline{1})\}.$$

If there is a group homomorphism $f : \mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2$, then f is injective, and so $ord(x) = ord(f(x))$ for every $x \in \mathbb{Z}_4$ by Ex. 9.

But $ord(z_1) = 4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$ has no element of order 4. Hence, these groups can't be isomorphic.