8 Tutorial 8 – November 21st, 2017

8.1 A revision exercise. Find all $x \in \mathbb{Z}_{501}$ for which

$$51\,x = 36,$$

where the multiplication is in $\mathbb{Z}_{501}$.

8.2 A revision exercise. Find the remainder when we divide the number 101^{49} by 23.

8.3 A revision exercise. On the set $A = \mathbb{Q} \setminus \{0\}$ an operation $\circ$ is given by

$$x \circ y = \frac{1}{\frac{1}{x} + \frac{1}{y}}.$$

Decide whether $(A, \circ)$ is a semigroup, and whether it has a neutral element.

8.4 Given a group $(\mathbb{Z}_{11}^\star, \cdot, 1)$ of all invertible elements of $(\mathbb{Z}_{11}, \cdot, 1)$. Show that it is a cyclic group. Find at least one generating element. How many generating elements $(\mathbb{Z}_{11}^\star, \cdot, 1)$ has?

Solution. A group is cyclic if and only if it has a generating element; i.e. an element $a \in \mathbb{Z}_{11}^\star$ such that any element of $\mathbb{Z}_{11}^\star$ is a power of a. Let us try "small"elements a (the reason for that is that it is easier to calculate the powers of small number than "bigger"ones).

For $a = 2$ we have

- $a^1 = 2$;
- $a^2 = 2^2 = 4$;
- $a^3 = 2^3 = 8 = -3$;
- $a^4 = 2^4 = 5$;
- $a^5 = 2^5 = 10 = -1$;
- $a^6 = 2^6 = -2 = 9$;
- $a^7 = 2^7 = -4 = 7$;
- $a^8 = 2^8 = 3$;
- $a^9 = 2^9 = -5 = 6$;
- $a^{10} = 2^{10} = 1$.

We can see that all 10 elements of $\mathbb{Z}_{11}^\star$ are powers of 2, hence 2 is a generating element of $(\mathbb{Z}_{11}^\star, \cdot 1)$. Therefore, $(\mathbb{Z}_{11}^\star, \cdot 1)$ is a cyclic group.

Since any element $b = 2^i$ with $\gcd(i, 10) = 1$ is also a generating element of $(\mathbb{Z}_{11}^\star, \cdot 1)$, there are $\phi(10) = 4$ generating elements. The generating elements are $6 = 2^9$, $7 = 2^7$ a $8 = 2^3$.

Let us mention that we do not have to calculate all the powers of 2. Indeed, the order of any element of a finite group divides the order of the group. Hence, $a \in \mathbb{Z}_{11}^\star$ can have orders only one of the numbers 1, 2, 5, 10 (which are divisors of $10 = |\mathbb{Z}_{11}^\star|$). Therefore, if $a \neq 1$ satisfies $a^2 \neq 1$, $a^5 \neq 1$, then a is a generating element of $(\mathbb{Z}_{11}^\star, \cdot 1)$.

8.5 Given a group $(\mathbb{Z}_8^\star, \cdot, 1)$ of all invertible elements of $(\mathbb{Z}_8, \cdot, 1)$. Decide whether it is a cyclic group.

Solution. We have $a \in \mathbb{Z}_8^\star$ if and only if $\gcd(a, 8) = 1$. Hence $\mathbb{Z}_8^\star = \{1, 3, 5, 7\}$. Let us calculate orders of all elements of $\mathbb{Z}_8^\star$.

- The order of 1 is 1.
- Since $3^2 = 1$, the order of 3 is 2.

- Since $5^2 = 1$, the order of 5 is 2.
- Since $7^2 = 1$, the order of 7 is 2.

Hence, all elements of $\mathbb{Z}_8^\star$ different from 1 have order 2, no one has order 4. Therefore, $(\mathbb{Z}_8^\star, \cdot, 1)$ is not cyclic.

Notice that $(\mathbb{Z}_8^\star, \cdot, 1)$ has 5 subgroups: namely, $\{1\}$, $\{1,3\}$, $\{1,5\}$, $\{1,7\}$, and $\mathbb{Z}_8^\star$. Unlike a cyclic group $(\mathbb{Z}_8^\star, \cdot, 1)$ has three subgroups for order 2.

8.6 Given a group $(\mathbb{Z}_{17}^\star, \cdot, 1)$. Find the order of 2. Is 2 a generating element? Write down $\langle 2 \rangle$ in $\mathbb{Z}_{17}^\star$.

Solution. Since the group $(\mathbb{Z}_{17}^\star, \cdot, 1)$ has 16 elements, its elements have orders from the set of all divisors of 16, i.e. from the set $\{1, 2, 4, 8, 16\}$. We have $2^2 = 4$, $2^4 = 16 = -1$, hence $2^8 = 1$. Therefore, the order of 2 is 8. Since 2 has order 8, 2 is not a generator.

Moreover, $\langle 2 \rangle = \{2^i \mid 1 = 1, 2, 3, 4, 5, 6, 7, 8\} = \{1, 2, 4, 8, 9, 13, 15, 16\}$.

8.7 Given a group $(\mathbb{Z}_{17}^\star, \cdot, 1)$. Find all its generating elements.

Solution. From exercise 8.6 we know that $\langle 2 \rangle \neq \mathbb{Z}_{17}^\star$. Hence no $a \in \langle 2 \rangle$ is a generating element. Let us compute powers of 3:

- $3^2 = 9 \neq 1$;
- $3^4 = 13 = -4 \neq 1$;
- $3^8 = 16 = -1 \neq 1$.

Hence, the order of 3 is 16 and 3 is a generating element of $(\mathbb{Z}_{17}^\star, \cdot, 1)$.

There are $\phi(16) = 8$ generating elements; indeed, for every i relatively prime to 16, the element 3^i is a generating element. Hence, all generating elements are $3^1 = 3$, $3^3 = 10$, $3^5 = 5$, $3^7 = 11$, $3^9 = 14$, $3^{11} = 7$, $3^{13} = 12$ a $6 = 3^{15}$.

8.8 Given a group $(\mathbb{Z}_{17}^\star, \cdot, 1)$. Find all its subgroups.

Solution. Since the group $(\mathbb{Z}_{17}^\star, \cdot, 1)$ is a cyclic group with 16 elements, for every divisor d of 16 there is one subgroup of d elements.

1. For $d = 1$, we have the subgroup $\{1\}$.
2. For $d = 2$, we have the subgroup $\{1, -1\} = \{1, 16\}$; indeed, $16 = -1$ has order 2.
3. For the subgroup with 4 elements we need an element of order 4. Since 2 has the order 8, $2^2 = 4$ has the order 4. Hence $\langle 4 \rangle = \{4, 4^2, 4^3, 4^4\}$ is the subgroup of order 4. Moreover, $4^2 = 16 = -1$, $4^3 = -4 = 13$, and $4^4 = 1$. Hence $\langle 4 \rangle = \{1, 4, 13, 16\}$.
4. We already know that $\langle 2 \rangle$ has 8 elements, so the set $\{1, 2, 4, 8, 9, 13, 15, 16\}$ forms a subgroup with 8 elements.
5. The only subgroup of $(\mathbb{Z}_{17}^\star, \cdot, 1)$ with 16 elements is $(\mathbb{Z}_{17}^\star, \cdot, 1)$ itself.

We have shown that $\{1\}$, $\{1, 16\}$, $\{1, 4, 13, 16\}$, $\{1, 2, 4, 8, 9, 13, 15, 16\}$ and $\mathbb{Z}_{17}^\star$ are all subgroups of $(\mathbb{Z}_{17}^\star, \cdot, 1)$.

Answers

8.1 $x_1 = 40$, $x_2 = 207$ a $x_3 = 374$

8.2 The remainder is 8.

8.3 The operation $\circ$ is an operation on the set $A = \mathbb{Q} \setminus \{0\}$ because for rational numbers x, y, $x \neq 0 \neq y$, the number $\frac{1}{\frac{1}{x}+\frac{1}{y}}$ is again a rational non-zero number.

Let us calculate

$$x \circ (y \circ z) = x \circ \frac{1}{\frac{1}{y}+\frac{1}{z}} = \frac{1}{\frac{1}{x}+\frac{1}{\frac{1}{y}+\frac{1}{z}}} = \frac{1}{\frac{1}{x}+\frac{1}{y}+\frac{1}{z}}.$$

On the other hand,

$$(x \circ y) \circ z = \frac{1}{\frac{1}{x}+\frac{1}{y}} \circ z = \frac{1}{\frac{1}{\frac{1}{x}+\frac{1}{y}}+\frac{1}{z}} = \frac{1}{\frac{1}{x}+\frac{1}{y}+\frac{1}{z}}.$$

Hence, $x \circ (y \circ z) = (x \circ y) \circ z$ and the operation $\circ$ satisfies the associativity law. Therefore, $(A, \circ)$ is a semigroup.

If e is a neutral element of $(A, \circ)$ then for every rational number $x \neq 0$ it must hold that

$$x \circ e = x = e \circ x.$$

So, $\frac{1}{\frac{1}{x}+\frac{1}{e}} = x$ for every x; which means that $\frac{1}{x} = \frac{1}{x} + \frac{1}{e}$. Hence $\frac{1}{e} = 0$, and this holds for no rational number. Therefore the neutral element does not exist.