Exercise 9 (Solutions)
28.11.2006

(1) We need to find all the integers \(0 < k < 6\) which are relatively prime to 6 = 2 \cdot 3. These are all \(k\) which are not a multiple of 2 or 3. These are: 1 and 5. Thus \(\mathbb{Z}_6\) has two generators.

We need to find all the integers \(0 < k < 8\) which are relatively prime to \(8 = 2^3\). These are all \(k\) which are not a multiple of 2. In this case they are: 1, 3, 5 and 7. Thus \(\mathbb{Z}_8\) has four generators.

We need to find all the integers \(0 < k < 12\) which are relatively prime to \(12 = 2^2 \cdot 3\). These are all \(k\) which are not a multiple of 2 or 3. These are: 1, 5, 7 and 11. Thus \(\mathbb{Z}_{12}\) has 4 generators.

We need to find all the integers \(0 < k < 60\) which are relatively prime to \(60 = 2^2 \cdot 3 \cdot 5\). In this case these are: 1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53 and 59. Thus \(\mathbb{Z}_{60}\) has 16 generators.

(2) We know that every subgroup of a cyclic group is again cyclic (Theorem 2.50). Thus we need just to show that every cyclic subgroup of \(\mathbb{Z}_p\) is a trivial subgroup of \(\mathbb{Z}_p\). Therefore let \(x \in \mathbb{Z}_p\) be an arbitrary element. If \(x = 0\) then \(\langle x \rangle = \{0\}\) is a trivial subgroup.

Therefore we may assume that \(x \neq 0\). Then \(0 < x < p\) and since \(p\) is a prime number it follows that \(x\) and \(p\) are relatively prime. Thus \(x\) is a generator of \(\mathbb{Z}_p\), that is \(\langle x \rangle = \mathbb{Z}_p\) is again a trivial subgroup of \(\mathbb{Z}_p\).

Alltogether every subgroup of \(\mathbb{Z}_p\) is relatively prime.

(3) There are two cases: (a) \(p = q\) and (b) \(p \neq q\).

(a) Possible candidates for generators is the set \(\mathbb{Z}_p^* := \{1, 2, \ldots, p^2 - 1\}\) which has \(p^2 - 1\) elements. An element \(x \in \mathbb{Z}_p^*\) is a generator of \(\mathbb{Z}_p^*\) if and only if it is relatively prime to \(p^2\). Thus \(x \in \mathbb{Z}_p^*\) is a generator only if it is not a multiple of \(p\). The multiples of \(p\) in the set \(\mathbb{Z}_p^*\) are

\[ p, 2p, 3p, 4p, \ldots, (p-2)p, (p-1)p \]

and these are \((p-1)\) different elements. Thus we have altogether \(\left|\mathbb{Z}_p^*\right| - (p-1) = p^2 - 1 - (p-1) = p^2 - p = p(p-1)\) generators for the group \(\mathbb{Z}_p^*\).

(b) Possible candidates for generators is the set \(\mathbb{Z}_{pq}^* := \{1, 2, \ldots, pq - 1\}\) which has \(pq - 1\) elements. Only elements in this set which are relatively prime to \(pq\) are generators of \(\mathbb{Z}_{pq}\). Thus every element in \(\mathbb{Z}_{pq}^*\) which is not a multiple of \(p\) or a multiples of \(q\). The multiples of \(p\) in \(\mathbb{Z}_{pq}^*\) are the \((q-1)\) elements

\[ p, 2p, 3p, 4p, \ldots, (q-2)p, (q-1)p \]

(and non of those elements can be a multiple of \(q\) since \(q\) and \(p\) are primes). Likewise the the multiples of \(q\) in \(\mathbb{Z}_{pq}^*\) are the \((p-1)\) elements

\[ q, 2q, 3q, 4q, \ldots, (p-2)q, (p-1)q \]

(and non of those elements can be a multiple of \(p\) since \(q\) and \(p\) are primes).
Thus we have altogether
\[
|\mathbb{Z}_{pq}^\times| = (q - 1)(p - 1) = pq - p - q + 1
\]
\[
= (p - 1)(q - 1)
\]
elements left which are then necessarily all generators of the group \(\mathbb{Z}_{pq}\).

(4) The elements of the group \(\mathbb{Z}_{36}\) are the following
\[
\mathbb{Z}_{36} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35\}
\]
• The generators of \(\mathbb{Z}_{36}\) are the elements which are relatively prime to \(36 = 2^2 \cdot 3^2\). This are all \(0 < k < 36\) which are not a multiple of 2 or 3, that is they are the following 12 elements
\[
1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35
\]
• It remains to study the following \(36 - 12 - 1 = 23\) elements
\[
2, 3, 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22, 24, 26, 27, 28, 30, 32, 33, 34
\]
which do not generate the whole group (and neither the trivial group \(\{0\}\)).
The group generated by 2 is
\[
\langle 2 \rangle = \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34\}
\]
and has 18 elements. Thus it is of the same type as \(\mathbb{Z}_{18}\).
Using the knowledge from the lecture notes about the group \(\mathbb{Z}_{18}\) we deduce the subgroup structure of \(\langle 2 \rangle \leq \mathbb{Z}_{36}\). The \(\mathbb{Z}_{18}\) has 4 non-trivial subgroups and there. Similarly \(\langle 2 \rangle\) has the four non-trivial subgroups (4), (6), (12) and (18).
• Thus we remain with the following \(23 - 17 = 6\) elements for discussion:
\[
3, 9, 15, 21, 27, 33.
\]
The subgroup generated by the element 3 is
\[
\langle 3 \rangle = \{0, 3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33\}
\]
and is of the same type as the group \(\mathbb{Z}_{12}\). From the first exercise we know that the group \(\mathbb{Z}_{12}\) has 4 generators. Thus also \(\langle 3 \rangle\) has 4 generators and those are 3, 15, 21 and 33.
• Thus we remain with the following \(6 - 4 = 2\) elements for discussion:
\[
9 \text{ and } 27. \text{ First we observe that since } 9 + 27 \equiv 0 \mod 36 \text{ it follows that } 9 \text{ and } 27 \text{ are inverse elements of each other under the addition modulo } 36. \text{ Therefore they generate the same subgroup, namely the subgroup }
\]
\[
\langle 9 \rangle = \{0, 9, 18, 27\}
\]
consisting of 4 elements.
Therefore we know now all subgroups of \(\mathbb{Z}_{36}\) and these are (beside the trivial ones): \(\langle 2 \rangle, \langle 3 \rangle, \langle 4 \rangle, \langle 9 \rangle, \langle 12 \rangle\) and \(\langle 18 \rangle\).
Its lattice diagram is

```
      Z_{36}
     /   \
    (2)   (3)
   / \   / \  
(4) (6) (9) 
  / \   / \  
(12) (18) 
   / \  
(0) 
```

(5) This is an application of Proposition 2.35.

(a) We have: $25 = 5^2$ and $30 = 2 \cdot 3 \cdot 5$. Thus $5 \in \gcd(30, 25)$ and $\text{ord}(25) = 30/5 = 6$.

(b) We have: $30 = 2 \cdot 3 \cdot 5$ and $42 = 2 \cdot 3 \cdot 7$. Thus $6 = 2 \cdot 3 \in \gcd(42, 30)$ and $\text{ord}(30) = 42/6 = 7$.

(c) We have: $25 = 5^2$ and $42 = 2 \cdot 3 \cdot 7$. Thus $1 \in \gcd(42, 25)$ and $\text{ord}(25) = 42/1 = 42$. That is $25$ is a generator of $\mathbb{Z}_{42}$.

(6*) From the literature\(^1\) one gets the following factorisation of $|M|$ into prime numbers:

$$|M| = 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$$

Using this information we can then solve the exercise.

(a) We have $323 = 17 \cdot 19$. Thus $323$ is a factor of $|M|$ and it follows that $323 \in \gcd(|M|, 323)$. Then $\text{ord}(323) = |M|/323 \approx 2.5 \cdot 10^{31}$.

(b) Since $37$ is not a prime factor of $|M|$ it follows that $|M|$ and $37$ are relatively prime. Thus $37$ is a generator of $G$.

\(^1\)For example http://en.wikipedia.org/wiki/Monster_group