MA1214

Introduction to group theory

Prof. Zaitsev

Solutions to Sheet 6

leitner@stp.dias.ie

1. Euclidean algorithm

(a)

$$\gcd(1001, 33) = \gcd(1001 - \underbrace{30 \cdot 33}_{=990}, 33) = \gcd(11, 33) = 11 \,.$$

$$11 = 1001 - 30 \cdot 33 \,.$$

(b)

$$\gcd(56, 126) = gcd(56, 126 - \underbrace{2 \cdot 56}_{=112}) = (\underbrace{56}_{=4\cdot 14}, 14) = 14 \,.$$

$$14 = -2 \cdot 56 + 126$$

(c)

$$\gcd(234, 2341) = gcd(234, 2341 - \underbrace{10 \cdot 234}_{=2340}) = \gcd(234, 1) = 1 \,.$$

$$1 = -10 \cdot 234 + 2341$$

2. Let $\mathfrak{P}$ be the set of prime numbers. Suppose

$$a = \prod_{\substack{p\in\mathfrak{P} \\ \text{almost all } n(p)=0}} p^{n(p)}$$

$$b = \prod_{\substack{p\in\mathfrak{P} \\ \text{almost all } m(p)=0}} p^{m(p)}$$

$$c = \prod_{\substack{p\in\mathfrak{P} \\ \text{almost all } k(p)=0}} p^{k(p)}$$

(a) For a, b as above, we have

$$\gcd(a, b) = \prod_{\substack{p\in\mathfrak{P} \\ \text{almost all } n(p),m(p)=0}} p^{\min(n(p),m(p))} \,.$$

Now for a, b, c as above,

$$ac = \prod_{\substack{p\in\mathfrak{P} \\ \text{almost all } n(p),k(p)=0}} p^{n(p)+k(p)}$$

$$\gcd(ac, bc) = \prod_{\substack{p\in\mathfrak{P} \\ \text{almost all } n(p),m(p),k(p)=0}} p^{\min(n(p)+k(p),m(p)+k(p))}$$

On the other hand,

$$c\gcd(a,b) = \prod_{\substack{p\in\mathfrak{P}\\ \text{almost all } k(p)=0}} p^{k(p)} \prod_{\substack{p\in\mathfrak{P}\\ \text{almost all } n(p),m(p)=0}} p^{\min(n(p),m(p))}$$

It suffices to show that (abbreviating notations) for $k = k(p)$, $n = n(p)$, $m = m(p)$, we have

Claim 1.

$$\min(n+k, m+k) = \min(n,m) + k\,.$$

Proof. We have

$$n+k \le m+k \quad \Leftrightarrow \quad n \le m$$

Suppose w.l.o.g. $n \le m$, i.e. $\min(n,m) = n$. Then

$$\min(n+k, m+k) = n+k = \min(n,m) + k\,.$$

□

(b) Let

$$a = p_1 \dots p_n\,, \quad b = q_1, \dots, q_m\,, \quad c = r_1 \dots, r_k\,,$$

where for $1 \le i \le n$, $1 \le j \le m$, $1 \le \ell \le k$, we have $p_i, q_j, r_\ell \in \mathfrak{P}$.

- Suppose $\gcd(a,c) = \gcd(p_1 \dots p_n, r_1 \dots r_k) = 1$. Then no prime r_j equals any of the primes p_i.
  (For suppose $\exists$ pair (i,j) s.t. $p_i = r_j$. Then

  $$\gcd(a,c) = p_i \gcd(p_1 \dots p_{i-1} p_{i+1} \dots p_n, r_1 \dots r_{j-1} r_{j+1} \dots r_k)$$

  by part 2a. But $\gcd(a,c) = 1$ so we must have

  $$p_i = \pm 1 \quad \text{and} \quad \gcd(p_i^{-1} a, r_j^{-1} c) = \pm 1\,.$$

  Contradiction, since ± 1 is not a prime number.)
- Suppose $\gcd(b,c) = \gcd(q_1 \dots q_m, r_1 \dots r_k) = 1$. Then no prime r_j equals any of the primes q_i.
- $\gcd(ab,c) = \gcd(p_1 \dots p_n q_1 \dots q_m, r_1 \dots r_k) = 1$ since no prime r_j equals any of the primes p_i, or any of the primes q_i.

3. (a) The set

$$\mathbb{Z}_8 = \mathbb{Z}/8\mathbb{Z} = \{[0],[1],[2],[3],[4],[5],[6],[7]\}$$

is a cyclic group w.r.t. +, generated by [1]. Let $H := \langle [4] \rangle \subset \mathbb{Z}_8$. As a set,

$$H = \{[0],[4]\}\,.$$

A left coset of H in $\mathbb{Z}_8$ is the set $g + H = \{g + h | h \in H\}$ for some $g \in \mathbb{Z}_8$. We have

$$\begin{aligned}
\mathbb{Z}_8 + [0] &= \mathbb{Z}_8 \\
[0] + [4] &= [4] \\
[1] + [4] &= [5] \\
[2] + [4] &= [6] \\
[3] + [4] &= [7] \\
[4] + [4] &= [8] = [0] \\
[5] + [4] &= [9] = [1] \\
[6] + [4] &= [10] = [2] \\
[7] + [4] &= [11] = [3] \, .
\end{aligned}$$

Addition is commutative, so there is no need to set up a second list for the right cosets: left and right cosets are equal. All cosets are

$$\begin{aligned}
[0] + H &= \{[0], [4]\} = [4] + H = H \\
[1] + H &= \{[1], [5]\} = [5] + H \\
[2] + H &= \{[2], [6]\} = [6] + H \\
[3] + H &= \{[3], [7]\} = [7] + H \, .
\end{aligned}$$

Note: Different cosets have no common element. The identity is contained in the coset H.

(b) The set

$$S_3 = \{(1), (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$$

(endowed with the composition $\circ$) is the group of permutations of three elements. Let $H := \langle(1\ 2)\rangle \subset S_3$. As a set,

$$H = \{(1), (1\ 2)\} \, .$$

Though this is not made explicit, the point of the exercise is to list actually *all* left and all right cosets (since it turns out that there are only three for either side).

- A *left coset* of H in S_3 is the set $g \circ H = \{g \circ h | h \in H\}$ for some $g \in S_3$. We have

$$\begin{aligned}
S_3(1) &= S_3 \\
(1)(1\ 2) &= (1\ 2) \\
(1\ 2)(1\ 2) &= (1\ 2)^2 = (1) \\
(1\ 3)(1\ 2) &= (1\ 2\ 3) \\
(2\ 3)(1\ 2) &= (1\ 3\ 2) \\
(1\ 2\ 3)(1\ 2) &= (1\ 3) \\
(1\ 3\ 2)(1\ 2) &= (2\ 3) \, ,
\end{aligned}$$

  (cf. sheet 4, problem 2). Thus the *left cosets* of H in S_3 are

$$\begin{aligned}
(1)H &= \{(1), (1\ 2)\} = (1\ 2)H = H \\
(1\ 3)H &= \{(1\ 3), (1\ 2\ 3)\} = (1\ 2\ 3)H \\
(2\ 3)H &= \{(2\ 3), (1\ 3\ 2)\} = (1\ 3\ 2)H \, .
\end{aligned}$$

- A *right coset* of H in S_3 is the set $H \circ g = \{h \circ g | h \in H\}$ for some $g \in S_3$. We have

$$\begin{aligned}
(1)S_3 &= S_3 \\
(1\,2)(1) &= (1\,2) \\
(1\,2)(1\,2) &= (1\,2)^2 = (1) \\
(1\,2)(1\,3) &= (1\,3\,2) \\
(1\,2)(2\,3) &= (1\,2\,3) \\
(1\,2)(1\,2\,3) &= (2\,3) \\
(1\,2)(1\,3\,2) &= (1\,3)\,.
\end{aligned}$$

  Thus the *right cosets* of H in S_3 are

$$\begin{aligned}
H(1) &= \{(1), (1\,2)\} = H(1\,2) = H \\
H(1\,3) &= \{(1\,3), (1\,3\,2)\} = H(1\,3\,2) \\
H(2\,3) &= \{(2\,3), (1\,2\,3)\} = H(1\,2\,3)\,.
\end{aligned}$$

  Note: Left and right cosets of the same element $g \in S_3$ are in general different sets.

(c) Let $H \subseteq G$ be a subgoup (in particular a group itself).

- Suppose $g \in H$. Then $gH \subseteq H$ since H is closed under multiplication. We also have $gH \supseteq H$ (every element is reached by the multiplication with g): Given any $h' \in H$, we have $gh = h'$ for $h = g^{-1}h' \in H$:

$$gh = g(g^{-1}h') = (gg^{-1})h' = eh' = h'\,.$$

  We have shown that for $g \in H$, we have $gH = H$.
- Inversely, suppose $gH = H$. Choosing $e \in H$ yields $ge = g$, so $g \in H$.

This completes the proof.