ETH Zürich, D-INFK
HS 2020, 18. November 2020

Prof. Ueli Maurer
David Lanzenberger

Diskrete Mathematik

Solution 9

9.1 Structure of Groups

a) There are 6 subgroups:

$$\{(0,0)\}, \quad \{0,2\} \times \{0\}, \quad \mathbb{Z}_4 \times \{0\}, \quad \{0\} \times \mathbb{Z}_5, \quad \{0,2\} \times \mathbb{Z}_5, \quad \mathbb{Z}_4 \times \mathbb{Z}_5$$

You are not required to formally justify why these are all subgroups.

b) Take arbitrary $a, b \in G$. Since $a * a = e$ and $b * b = e$, we have $a = \widehat{a}$, $b = \widehat{b}$ and $a * b = \widehat{a * b}$. Hence, $a * b = \widehat{a * b} \overset{\text{Lemma 5.3}}{=} \widehat{b} * \widehat{a} = b * a$.

9.2 Isomorphisms Map Generators to Generators

Take an arbitrary $h \in H$ and let $a = \psi^{-1}(h)$ (the inverse of ψ exists, because ψ is bijective). Since g is a generator, there exists an $m \in \mathbb{Z}$ such that $a = g^m$.

- If $m = 0$, then by Lemma 5.5 (i), $h = \psi(g^0) = \psi(e) = e' = \psi(g)^0$, where e and e' are the neutral elements of G and H, respectively.
- If $m > 0$, then $h = \psi(g^m) = \psi(g)^m$, where the last step is trivial for $m = 1$ and otherwise follows from applying the definition of a homomorphism $m - 1$ times.
- If $m < 0$, then $h = \psi(g^m) = \psi((\widehat{g})^{|m|}) = \psi(\widehat{g})^{|m|} = (\widetilde{\psi(g)})^{|m|} = \psi(g)^m$, where the third step is justified as above, and the fourth step follows from Lemma 5.5 (ii).

9.3 Applying Group Elements to Elements of Arbitrary Sets

a) For any $s \in S$ we can choose $s' = \theta(\widehat{a}, s)$ to obtain

$$\begin{aligned}
\psi_a(s') &= \psi_a(\theta(\widehat{a}, s)) && \text{(def. } s'\text{)} \\
&= \theta(a, \theta(\widehat{a}, s)) && \text{(def. } \psi_a\text{)} \\
&= \theta(a * \widehat{a}, s) && \textbf{ii)} \\
&= \theta(e, s) && \text{(G3)} \\
&= s. && \textbf{i)}
\end{aligned}$$

This proves that ψ_a is surjective. Moreover, we have for any $s, s' \in S$

$$\begin{aligned}
\psi_a(s) = \psi_a(s') &\implies \theta(a, s) = \theta(a, s') && \text{(def. } \psi_a\text{)} \\
&\implies \theta(\widehat{a}, \theta(a, s)) = \theta(\widehat{a}, \theta(a, s')) \\
&\implies \theta(\widehat{a} * a, s) = \theta(\widehat{a} * a, s') && \textbf{ii)} \\
&\implies \theta(e, s) = \theta(e, s') && \text{(G3)} \\
&\implies s = s'. && \textbf{i)}
\end{aligned}$$

Hence, ψ_a is also injective, and thus bijective.

b) We prove that $\sim$ satisfies all properties of an equivalence relation.

Reflexivity: For any $s \in S$, **i)** implies that $\theta(e, s) = s$, so we have $s \sim s$.

Symmetry: For any $s, t \in S$ we have

$$\begin{aligned}
s \sim t &\implies \theta(a, s) = t \text{ for some } a \in G && \text{(def. } \sim\text{)} \\
&\implies \theta(\widehat{a}, \theta(a, s)) = \theta(\widehat{a}, t) \text{ for some } a \in G \\
&\implies \theta(\widehat{a} * a, s) = \theta(\widehat{a}, t) \text{ for some } a \in G && \textbf{ii)} \\
&\implies \theta(e, s) = \theta(\widehat{a}, t) \text{ for some } a \in G && \text{(G3)} \\
&\implies s = \theta(\widehat{a}, t) \text{ for some } a \in G && \textbf{i)} \\
&\implies \theta(a, t) = s \text{ for some } a \in G \\
&\implies t \sim s \text{ for some } a \in G. && \text{(def. } \sim\text{)}
\end{aligned}$$

Transitivity: For any $s, t, v \in S$ we have

$$\begin{aligned}
s \sim t \text{ and } t \sim v &\implies \theta(a, s) = t \text{ and } \theta(b, t) = v \text{ for some } a, b \in G && \text{(def. } \sim\text{)} \\
&\implies \theta(b, \theta(a, s)) = v \text{ for some } a, b \in G && \text{(substituting } t\text{)} \\
&\implies \theta(b * a, s) = v \text{ for some } a, b \in G && \textbf{ii)} \\
&\implies \theta(a, s) = v \text{ for some } a \in G \\
&\implies s \sim v. && \text{(def. } \sim\text{)}
\end{aligned}$$

9.4 Rotations of a Cube

a) First of all, one has to decide which corner of the sofa coincides with the corner of the room. For this, there are 8 possibilities. Once this corner is set, there are 3 edges coming out of this corner (one of them going up) and, hence, 3 possibilities to place the sofa. Once the corner and the edge going up are fixed, the position of the sofa is fully defined. Hence, there are $3 \cdot 8 = 24$ possibilities overall.

b) Let us first determine $|R|$. Assume that the sofa stands in the corner in a certain (arbitrary) position. After a rotation b, it may end up in one of the 24 possible positions (this follows from Subtask a)). Therefore, we can distinguish 24 different rotations and $|R| = 24$.

It is possible to describe each element of R as a rotation around single axis. To see this, consider all possible different rotations of a cube around an axis:

- Identity.
- Rotation around the centers of two opposite faces. There are 3 pairs of opposite faces and for each pair there are 3 possible rotations: by 90, 180 and 270 degrees. Together, this gives 9 rotations.
- Rotation around two opposite vertices. There are 4 pairs of opposite vertices and for each pair there are 2 possible rotations: by 120 and 240 degrees. Together, this gives 8 rotations
- Rotation around the centers of two opposite edges. There are 6 pairs of opposite edges and for each pair there is only one possible rotation: by 180 degrees. Together, this gives 6 rotations.

One can see (for example by drawing the cube after each rotation) that no two of the above rotations end up with the cube being in the same position. Since together we described 24 rotations and $|R| = 24$, each element of R corresponds to *exactly one* rotation.

c) $\langle R; \circ \rangle$ is a group. Since function composition is associative, $\circ$ is associative as well (this is because every rotation corresponds to a permutation of vertices). The neutral element is the identity. Furthermore, every element has an inverse, namely a rotation around the same axis by 360 degrees minus the original angle.

d) The operation $\circ$ is not commutative. Figure 1 illustrates that there exist rotations, which do not commute.

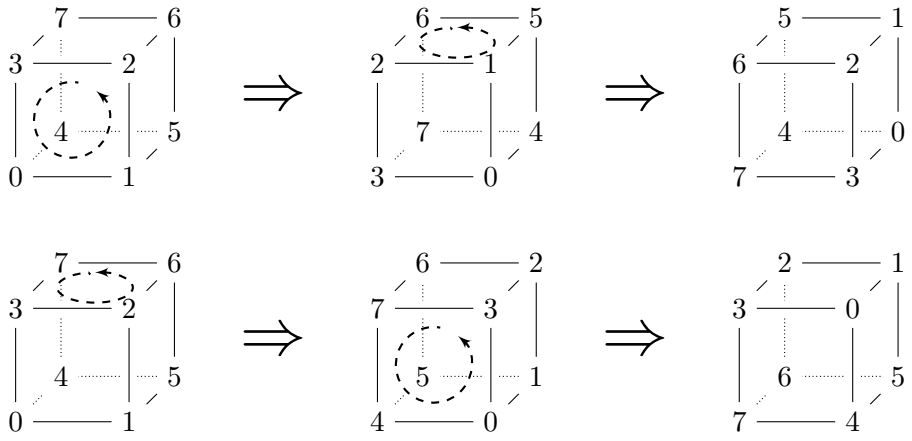

Figure 1: $\langle R; \circ \rangle$ is not commutative.

9.5 Diffie-Hellman

a) Let $g \in \langle \mathbb{Z}_n; \oplus \rangle$ be the generator, which Alice and Bob use as the basis. Alice chooses x_A at random from $\{0, \ldots, n-1\}$ and sends $y_A = R_n(g \cdot x_A)$. Analogously, Bob chooses x_B at random from $\{0, \ldots, n-1\}$ and sends $y_B = R_n(g \cdot x_B)$. The established shared key is $k_{AB} = R_n(g \cdot x_A \cdot x_B)$.

As shown in Example 5.27, we have $\gcd(g, n) = 1$. Therefore, Eve can use the Extended GCD algorithm to efficiently find an $a \in \mathbb{Z}$ such that $a \cdot g \equiv_n 1$. Then she can compute k_{AB} using the eavesdropped messages y_A and y_B as $k_{AB} = R_n(a \cdot y_A \cdot y_B)$. This is because

$$k_{AB} \equiv_n g \cdot x_A \cdot x_B \equiv_n g \cdot x_A \cdot (a \cdot g) \cdot x_B \equiv_n a \cdot (g \cdot x_A) \cdot (g \cdot x_B) \equiv_n a \cdot y_A \cdot y_B$$

b) Let us make Bob's argument more explicit: The Diffie-Hellman protocol using a cyclic group $G = \langle g \rangle$ is insecure if the discrete logarithm problem in G is easy. Since by Theorem 5.7 there exists an isomorphism $\varphi : G \to \mathbb{Z}_n$, one can compute x such that $g^x = h$ by instead computing x such that $\varphi(g)^x = \varphi(h)$. Since this can be done efficiently (both $\varphi(g)$ and $\varphi(h)$ are in $\mathbb{Z}_n$), Bob concludes that the discrete logarithm problem is easy in all cyclic groups.

Bob's argument is incorrect, because the above procedure is efficient only if the isomorphism φ can be efficiently computed, which is not always the case. For example, computing the isomorphism given in the proof of Theorem 5.7 requires solving the discrete logarithm problem in G (so Bob's procedure would give no advantage).

9.6 The Group $\mathbb{Z}_m^*$

a) The order of the group $\langle \mathbb{Z}_{36}^*; \odot \rangle$ is $\varphi(36)$. By Lemma 5.12,

$$\varphi(36) = (2-1) \cdot 2^{2-1} \cdot (3-1) \cdot 3^{2-1} = 2 \cdot 2 \cdot 3 = 12.$$

$\mathbb{Z}_{36}^*$ consists of all numbers in $\mathbb{Z}_{36}$ which are relatively prime with 36, that is, $\mathbb{Z}_{36}^* = \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\}$.

b) We will verify for each $a \in \mathbb{Z}_{11}^*$ whether it is a generator (but more efficiently than by computing $\langle a \rangle$). An $a \in \mathbb{Z}_{11}^*$ is a generator if and only if $\mathrm{ord}(a) = 10$. By Lagrange's Theorem, $\mathrm{ord}(a) \in \{1, 2, 5, 10\}$, so a is a generator if and only if $\mathrm{ord}(a) \notin \{1, 2, 5\}$, that is, if and only if $a \neq 1$, $a^2 \neq 1$ and $a^5 \neq 1$. We can now compute $R_{11}(a^2)$ and $R_{11}(a^5)$ for all $a \in \{2, \ldots, 10\}$. The generators are $2, 6, 7$ and 8.

Note. Another way to solve this exercise for any $\langle \mathbb{Z}_m^*; \odot \rangle$ is to first use Theorem 5.15 to determine whether $\langle \mathbb{Z}_m^*; \odot \rangle$ is cyclic. If so, it is isomorphic to $\langle \mathbb{Z}_{\varphi(m)}; \oplus \rangle$. Now we find one generator g of $\mathbb{Z}_m^*$ (by trying all possibilities) and prove that for any $i \in \mathbb{Z}_{\varphi(m)}$, g^i is a generator if and only if $\gcd(i, \varphi(m)) = 1$ (see Example 5.27).

c) We prove that $f : \mathbb{Z}_{nm}^* \to \mathbb{Z}_n^* \times \mathbb{Z}_m^*$, defined by $f(x) = (R_n(x), R_m(x))$ is an isomorphism. Throughout the proof we will use the fact that $\gcd(R_m(x), m) = \gcd(x, m)$ for any x, m, which follows from Lemma 4.2.

f is a function. We show that $f(x) \in \mathbb{Z}_n^* \times \mathbb{Z}_m^*$ for all $x \in \mathbb{Z}_{nm}^*$.

Let $x \in \mathbb{Z}_{nm}^*$, which means that $\gcd(x, nm) = 1$. Let $d = \gcd(x, n)$. Then, $d \mid x$ and $d \mid n$, which implies that $d \mid x$ and $d \mid nm$, so by the definition of $\gcd$, $d \mid \gcd(x, nm)$. Hence, $d \mid 1$, so $d = 1$. Therefore, $\gcd(R_n(x), n) = \gcd(x, n) = 1$, so $R_n(x) \in \mathbb{Z}_n^*$.

The proof that $R_m(x) \in \mathbb{Z}_m^*$ is analogous.

f **is surjective.** Take any $(a, b) \in \mathbb{Z}_n^* \times \mathbb{Z}_m^*$. Since $\gcd(m, n) = 1$, by CRT, there exists an $x \in \mathbb{Z}_{nm}$ such that $(R_n(x), R_m(x)) = (a, b)$. To show that $x \in \mathbb{Z}_{nm}^*$, assume towards a contradiction that $d = \gcd(x, nm) > 1$. Let p be an arbitrary prime in the decomposition of d. Since $p \mid mn$, by Lemma 4.7, $p \mid n$ or $p \mid m$. In the first case, since also $p \mid x$, we get $p \mid \gcd(x, n)$. But $\gcd(x, n) = \gcd(R_n(x), n) = \gcd(a, n) = 1$ (because $a \in \mathbb{Z}_n^*$), so this is a contradiction. Analogously, in the second case we get $p \mid \gcd(b, m)$.

f **is injective.** By CRT, the x defined above is unique in $\mathbb{Z}_{nm}$, hence, it is also unique in $\mathbb{Z}_{nm}^*$.

f **is a homomorphism.** For any $a, b \in \mathbb{Z}_{nm}^*$,

$$\begin{aligned}
f(a \odot_{nm} b) =& (R_n(a \odot_{nm} b), R_m(a \odot_{nm} b)) \\
=& (R_n(R_{nm}(ab)), R_m(R_{nm}(ab))) \\
=& (R_n(ab),\ R_m(ab)) \\
=& (R_n(R_n(a) \cdot R_n(b)),\ R_m(R_m(a) \cdot R_m(b))) \\
=& (R_n(a) \odot_n R_n(b),\ R_m(a) \odot_m R_m(b)) \\
=& (R_n(a), R_m(a)) \star (R_n(b), R_m(b))\ ^1 \\
=& f(a) \star f(b).
\end{aligned}$$

d) The goal is to construct an isomorphism $\varphi : \mathbb{Z}_{15}^* \to \mathbb{Z}_{20}^*$. We will proceed in three steps, where we construct three isomorphisms: $\alpha : \mathbb{Z}_{15}^* \to \mathbb{Z}_3^* \times \mathbb{Z}_5^*$, $\beta : \mathbb{Z}_3^* \times \mathbb{Z}_5^* \to \mathbb{Z}_4^* \times \mathbb{Z}_5^*$ and $\gamma : \mathbb{Z}_4^* \times \mathbb{Z}_5^* \to \mathbb{Z}_{20}^*$. We then define φ as the composition of these isomorphisms: $\varphi = \gamma \circ \beta \circ \alpha$.

To construct α, we use Subtask a) and define $\alpha : a \mapsto (R_3(a), R_5(a))$. Further, let f be the isomorphism $f : \mathbb{Z}_{20}^* \to \mathbb{Z}_4^* \times \mathbb{Z}_5^*$, defined by $f : a \mapsto (R_4(a), R_5(a))$. We set $\gamma = f^{-1}$ (γ can be computed efficiently using the Chinese Remainder Theorem).

What is left is to find the isomorphism β. Note first that the function $g : \mathbb{Z}_3^* \to \mathbb{Z}_4^*$ defined by $g(1) = 1$ and $g(2) = 3$ is an isomorphism. The function g is trivially bijective. We also have $g(1 \odot 1) = 1 = g(1) \odot g(1)$, $g(2 \odot 1) = 3 = g(2) \odot g(1)$, $g(1 \odot 2) = 3 = g(1) \odot g(2)$ and $g(2 \odot 2) = 1 = g(2) \odot g(2)$. Therefore, g is also a homomorphism. Therefore, β defined by $\beta\big((a, b)\big) = \big(g(a), b\big)$ is an isomorphism.

Note. Alternatively, one can find an isomorphism ψ using trial and error. However, in such case one has to prove that ψ is indeed an isomorphism.

9.7 An RSA Attack

First, consider the case when n_1, n_2 and n_3 are not relatively prime. Without loss of generality, assume that $\gcd(n_1, n_2) > 1$. We can now use the Extended GCD algorithm to compute $p = \gcd(n_1, n_2)$ and this way efficiently factorize n_1. This allows us to compute the secret key of Alice and decrypt c_1.

[1] The operation $\star$ on $\mathbb{Z}_n^* \times \mathbb{Z}_m^*$ is defined as $(a_1, b_1) \star (a_2, b_2) := (a_1 \odot_n a_2,\ b_1 \odot_m b_2)$.

Secondly, assume that n_1, n_2 and n_3 are relatively prime. Consider the following system of congruence equations:

$$\begin{aligned} x &\equiv c_1 \pmod{n_1} \\ x &\equiv c_2 \pmod{n_2} \\ x &\equiv c_3 \pmod{n_3} \end{aligned}$$

Let $N = n_1 n_2 n_3$. Using the Chinese Remainder Theorem, we can efficiently find the solution x_0 to the above system of equations, such that $0 \leq x_0 < N$.

Notice now that m^3 is also a solution to the system of equations, because $c_i \equiv m^3 \pmod{n_i}$ for $i \in \{1, 2, 3\}$. Moreover, since $0 \leq m < n_i$ for $i \in \{1, 2, 3\}$, we have $0 \leq m^3 < n_1 \cdot n_2 \cdot n_3 = N$. Since by the Chinese Remainder Theorem x_0 is unique in $\{0, \ldots, N-1\}$, it follows that $x_0 = m^3$.

What is left is to compute the cube root of x_0 over $\mathbb{Z}$, which can be done efficiently.

Note. This attack is also possible for $e > 3$. However, for given e one needs e ciphertexts, each encrypted for a different recipient.