MIE-MPI: Tutorial 6

`created: October 29, 2019, 10:19`

6.1 Homomorphisms and isomorphisms

Exercise 6.1. Which of the following mappings are homomorphisms and which are isomorphisms from the given groups to the given groups?

(a) $\varphi(n) = 3n + 2$, from the group $(\mathbb{Z}, +)$ to $(\mathbb{R}, +)$;

(b) $\varphi(x) = 2^x$, from the group $(\mathbb{R}, +)$ to $(\mathbb{R}^+, \cdot)$;

(c) $\varphi(A) = A_{1,1}$, from the group of $n \times n$ matrices with the matrix addition (element-wise), denoted $(M, +)$, to $(\mathbb{R}, +)$;

(d) $\varphi(A) = A_{1,1}$, from the group of $n \times n$ regular with the matrix multiplication, denoted $(M_{\text{reg}}, \cdot)$, to $(\mathbb{R} \setminus \{0\}, \cdot)$.

Exercise 6.2. Find some homomorphism from $(M_{\text{reg}}, \cdot)$ to $(\mathbb{R} \setminus \{0\}, \cdot)$.

Exercise 6.3. Is $\mathbb{Z}_{10}^{\times}$ isomorphic with $\mathbb{Z}_5^{\times}$? If yes, find an isomorphism.

Exercise 6.4. How to find an isomorphism of groups $\mathbb{Z}_p^{\times}$ and $\mathbb{Z}_{p-1}^{+}$ in the general case? How many different isomorphisms exists?

6.2 Discrete logarithm

Exercise 6.5. Solve

$$5^x \equiv 12 \pmod{23}.$$

Exercise 6.6. Alice wants to send a secrete message to Bob during the MPI course[1]. So she sends a small paper via her classmates saying this:

> Hi Bobie, I am gonna send you a secrete message using Diffie-Hellman protocol.
> My public key is 29 and 8 and the encrypted stuff is 24.

Bob's answer is:

> Cool Alice! Mine is 15.

[1] Forgetting that the professor knows the trick too.

Alice:

> Super cool! Assuming that our shared secret number is n, let us meet on $(n-2 \mod 7)$-th day of the next week at $n-7$ o'clock in the cemetery in front of the tomb number $5n+6$. See ya!

Where and when are they going to meet?