

MATH 433

Applied Algebra

Lecture 31:

Isomorphism of groups (continued).

The ISBN code.

Isomorphism of groups

Definition. Let G and H be groups. A function $f : G \rightarrow H$ is called an **isomorphism** of the groups if it is bijective and $f(g_1g_2) = f(g_1)f(g_2)$ for all $g_1, g_2 \in G$.

The group G is said to be **isomorphic** to H if there exists an isomorphism $f : G \rightarrow H$.

Theorem Isomorphism is an equivalence relation on the set of all groups.

Theorem The following properties of groups are preserved under isomorphisms:

- the number of elements,
- being Abelian,
- being cyclic,
- having a subgroup of a particular order,
- having an element of a particular order.

Examples of isomorphic groups

- $(\mathbb{R}, +)$ and (\mathbb{R}_+, \times) .

An isomorphism $f : \mathbb{R} \rightarrow \mathbb{R}_+$ is given by $f(x) = e^x$.

- Any two cyclic groups $\langle g \rangle$ and $\langle h \rangle$ of the same order.

An isomorphism $f : \langle g \rangle \rightarrow \langle h \rangle$ is given by $f(g^n) = h^n$ for all $n \in \mathbb{Z}$.

- \mathbb{Z}_6 and $\mathbb{Z}_3 \times \mathbb{Z}_2$.

An isomorphism $f : \mathbb{Z}_6 \rightarrow \mathbb{Z}_3 \times \mathbb{Z}_2$ is given by $f([a]_6) = ([a]_3, [a]_2)$.

- $\mathbb{Z}_3 \times \mathbb{Z}_2$ and $\mathbb{Z}_2 \times \mathbb{Z}_3$.

An isomorphism $f : \mathbb{Z}_3 \times \mathbb{Z}_2 \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_3$ is given by $f([a]_3, [b]_2) = ([b]_2, [a]_3)$.

Examples of non-isomorphic groups

- $S(3)$ and \mathbb{Z}_7 .

$S(3)$ has order 6 while \mathbb{Z}_7 has order 7.

- $S(3)$ and \mathbb{Z}_6 .

\mathbb{Z}_6 is Abelian while $S(3)$ is not.

- \mathbb{Z} and $\mathbb{Z} \times \mathbb{Z}$.

\mathbb{Z} is cyclic while $\mathbb{Z} \times \mathbb{Z}$ is not.

- $\mathbb{Z} \times \mathbb{Z}$ and \mathbb{Q} .

$\mathbb{Z} \times \mathbb{Z}$ is generated by two elements $(1, 0)$ and $(0, 1)$ while \mathbb{Q} is not generated by a finite set.

Examples of non-isomorphic groups

- $\mathbb{Z} \times \mathbb{Z}_3$ and $\mathbb{Z} \times \mathbb{Z}$.

$\mathbb{Z} \times \mathbb{Z}_3$ has an element of finite order different from the identity element, e.g., $(0, [1]_3)$, while $\mathbb{Z} \times \mathbb{Z}$ does not.

- \mathbb{Z}_8 , $\mathbb{Z}_4 \times \mathbb{Z}_2$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

It follows from the classification of finite Abelian groups.

- $(\mathbb{R}, +)$ and $(\mathbb{R} \setminus \{0\}, \times)$.

Suppose $f : \mathbb{R} \setminus \{0\} \rightarrow \mathbb{R}$ is a homomorphism. Then $f(-1) + f(-1) = f((-1)(-1)) = f(1) = 0$, hence $f(-1) = 0 = f(1)$.

Error-detecting/correcting codes

Messages sent over electronic and other channels are subject to distortions of various sorts. Therefore it is important to encode a message so that a possible error can be detected. Then the receiver may ask that the message be repeated. Such codes are called **error-detecting**.

To achieve this, the message should carry a certain degree of redundancy. One way to do this is a **checksum**. Namely, the sender adds to a message one or several check symbols, which are functions of the message. Then the receiver reevaluates these additional symbols.

In some cases, requesting that the message be repeated is too expensive. For such cases, we need a code that not only can detect an error, but also allows to correct it. Such codes are called **error-correcting**.

ISBN

International Standard Book Number (ISBN) is assigned to all published books. It is an example of an error-detecting code.

- ISBN-10 (old standard) consists of 9 decimal digits that constitute the number followed by a check symbol, which is a digit in base 11 (0–9 or X, the Roman notation for 10).

If $a_1a_2 \dots a_9a_{10}$ is the number, then

$$10a_1 + 9a_2 + 8a_3 + \dots + 3a_8 + 2a_9 + a_{10}$$

is to be divisible by 11. This happens for a unique choice of a_{10} .

The code allows to detect one wrong digit or exchange of two digits.

Example. 0 521 54050 X (ISBN-10 of the textbook).

ISBN

- ISBN-13 (new standard) consists of 13 decimal digits, the last one being a checksum. If $b_1 b_2 \dots b_{12} b_{13}$ is the number, then $b_1 + 3b_2 + b_3 + 3b_4 + \dots + 3b_{12} + b_{13}$ is to be divisible by 10. This happens for a unique choice of b_{13} .

The code allows to detect one wrong digit or exchange of two neighboring digits.

Old numbers are converted into new ones by adding 978 at the beginning and recalculating the checksum.

Example. ISBN-10 of the textbook is 052154050X.

Therefore ISBN-13 of the textbook is 978-052154050d, where

$$\begin{aligned} &9 + 3 \cdot 7 + 8 + 3 \cdot 0 + 5 + 3 \cdot 2 + 1 \\ &+ 3 \cdot 5 + 4 + 3 \cdot 0 + 5 + 3 \cdot 0 + d \equiv 0 \pmod{10}. \end{aligned}$$

We obtain that $d = 6$.