MATH 433

Applied Algebra

Lecture 19:
Subgroups (continued).
Error-detecting and error-correcting codes.

Subgroups

Definition. A group H is a called a **subgroup** of a group G if H is a subset of G and the group operation on H is obtained by restricting the group operation on G.

Let S be a nonempty subset of a group G. The **group generated by** S, denoted $\langle S \rangle$, is the smallest subgroup of G that contains the set S. The elements of the set S are called **generators** of the group $\langle S \rangle$.

Theorem (i) The group $\langle S \rangle$ is the intersection of all subgroups of G that contain the set S.

(ii) The group $\langle S \rangle$ consists of all elements of the form $g_1 g_2 \dots g_k$, where each g_i is either a generator $s \in S$ or the inverse s^{-1} of a generator.

A **cyclic group** is a subgroup generated by a single element: $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$.

Lagrange's theorem

The number of elements in a group G is called the **order** of G and denoted $o(G)$. Given a subgroup H of G, the number of cosets of H in G is called the **index** of H in G and denoted $[G : H]$.

Theorem (Lagrange) If H is a subgroup of a finite group G, then $o(G) = [G : H] \cdot o(H)$. In particular, the order of H divides the order of G.

Corollary (i) If G is a finite group, then the order of any element $g \in G$ divides the order of G.
(ii) If G is a finite group, then $g^{o(G)} = 1$ for all $g \in G$. **(iii)** Any group G of prime order p is cyclic.

Subgroups of $\mathbb{Z}$

Integers $\mathbb{Z}$ with addition form a cyclic group, $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$. The proper cyclic subgroups of $\mathbb{Z}$ are: the trivial subgroup $\{0\} = \langle 0 \rangle$ and, for any integer $m \geq 2$, the group $m\mathbb{Z} = \langle m \rangle = \langle -m \rangle$. These are all subgroups of $\mathbb{Z}$.

Theorem Every subgroup of a cyclic group is cyclic as well.

Proof: Suppose that G is a cyclic group and H is a subgroup of G. Let g be the generator of G, $G = \{g^n : n \in \mathbb{Z}\}$. Denote by k the smallest positive integer such that $g^k \in H$ (if there is no such integer then $H = \{e\}$, which is a cyclic group). We are going to show that $H = \langle g^k \rangle$.

Take any $h \in H$. Then $h = g^n$ for some $n \in \mathbb{Z}$. We have $n = kq + r$, where q is the quotient and r is the remainder of n by k $(0 \leq r < k)$. It follows that $g^r = g^{n-kq} = g^n g^{-kq}$ $= h(g^k)^{-q} \in H$. By the choice of k, we obtain that $r = 0$. Thus $h = (g^k)^{-q} \in \langle g^k \rangle$.

- Subgroups of $(\mathbb{Z}_{10}, +)$.

The group is cyclic: $\mathbb{Z}_{10} = \langle [1] \rangle = \langle [3] \rangle = \langle [7] \rangle = \langle [9] \rangle$. It has three proper subgroups: the trivial subgroup $\{[0]\}$ (generated by [0]), a cyclic subgroup of order 2 $\{[0], [5]\}$ (generated by [5]), and a cyclic subgroup of order 5 $\{[0], [2], [4], [6], [8]\}$ (generated by either of the elements [2], [4], [6], and [8]).

- Subgroups of $(G_{15}, \times)$.

The group consists of 8 congruence classes modulo 15: $G_{15} = \{[1], [2], [4], [7], [8], [11], [13], [14]\}$. It is Abelian, but not cyclic. The cyclic subgroups of G_{15} are $\{[1]\}$, $\{[1], [4]\}$, $\{[1], [11]\}$, $\{[1], [14]\}$, $\{[1], [2], [4], [8]\}$, and $\{[1], [4], [7], [13]\}$. The only proper noncyclic subgroup is $\{[1], [4], [11], [14]\}$.

- Subgroups of $S(3)$.

The group consists of 6 permutations:
$S(3) = \{\mathrm{id}, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$. It is not Abelian. All proper subgroups of $S(3)$ are cyclic: $\{\mathrm{id}\}$, $\{\mathrm{id}, (1\ 2)\}$, $\{\mathrm{id}, (1\ 3)\}$, $\{\mathrm{id}, (2\ 3)\}$, and $\{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}$.

- Subgroups of $A(4)$.

The group consists of 12 permutations:

$$A(4) = \{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3)\}.$$

It is not Abelian. The cyclic subgroups are $\{\mathrm{id}\}$, $\{\mathrm{id}, (1\ 2)(3\ 4)\}$, $\{\mathrm{id}, (1\ 3)(2\ 4)\}$, $\{\mathrm{id}, (1\ 4)(2\ 3)\}$, $\{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}$, $\{\mathrm{id}, (1\ 2\ 4), (1\ 4\ 2)\}$, $\{\mathrm{id}, (1\ 3\ 4), (1\ 4\ 3)\}$, and $\{\mathrm{id}, (2\ 3\ 4), (2\ 4\ 3)\}$.
Also, $A(4)$ has one subgroup of order 4:
$\{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$.

Theorem The symmetric group $S(n)$ is generated by two permutations: $\tau = (1\ 2)$ and $\pi = (1\ 2\ 3\ \ldots\ n)$.

Proof: Let $H = \langle \tau, \pi \rangle$. We have to show that $H = G$.

First we obtain that $\alpha = \tau\pi = (2\ 3\ \ldots\ n)$. Then we observe that $\sigma(1\ 2)\sigma^{-1} = (\sigma(1)\ \sigma(2))$ for any permutation σ.
In particular, $(1\ k) = \alpha^{k-2}(1\ 2)(\alpha^{k-2})^{-1}$ for $k = 2, 3 \ldots, n$.
It follows that the subgroup H contains all transpositions of the form $(1\ k)$.

Further, for any integers $2 \leq k < m \leq n$ we have $(k\ m) = (1\ k)(1\ m)(1\ k)$. Therefore the subgroup H contains all transpositions. Finally, every permutation in $S(n)$ is a product of transpositions, therefore it is contained in H.

Remark. Although the group $S(n)$ is generated by two elements, its subgroups need not be generated by two elements.

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 achive 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 $a_1 a_2 \ldots a_9 a_{10}$ is the number, then

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

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 $b_1 + 3b_2 + b_3 + 3b_4 + \cdots + 3b_{12} + b_{13}$ 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

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

We obtain that $d = 6$.

Problem 1. Find the missing digit in an ISBN-10: 04*5011614.

Let d be the missing digit. Then

$$10 \cdot 0 + 9 \cdot 4 + 8d + 7 \cdot 5 + 6 \cdot 0 + 5 \cdot 1 + 4 \cdot 1 + 3 \cdot 6 + 2 \cdot 1 + 4 \equiv 0 \mod 11,$$

which simplifies to $8d + 5 \equiv 0 \mod 11$. The inverse of 8 modulo 11 is 7 (as $7 \cdot 8 = 56 \equiv 1 \mod 11$). It follows that $d \equiv 7 \cdot (-5) \equiv 9 \mod 11$. Thus $d = 9$.

Problem 2. Could this be a valid ISBN-13: 978-0495022613 ?

$$9 + 3 \cdot 7 + 8 + 3 \cdot 0 + 4 + 3 \cdot 9 + 5 + 3 \cdot 0 + 2 + 3 \cdot 2 + 6 + 3 \cdot 1 + 3 \equiv 4 \not\equiv 0 \mod 10,$$

therefore this could not be a valid ISBN-13.