31 August 2010

Syllabus on Leitzfried's webpage
a Blackboard page exists

First homework is posted.
It's a review of the lectures as a path through the book

The Idea of Algebra

descended from lectures of Noether & Co

- Geometric Symmetry
- Linear Algebra
- Polynomial Equations

Other Texts - Bibliography
- Lang (first edition has errors, but otherwise better)
- Van der Waerden
- M. Artin (for "undergraduates")
  a recombination of Van der Waerden
- Herstein ("undergraduate")
- Birkhoff - Maclane
- Jacobson
- Martin Isaacs (thin, zesty)

Homework
10-14 assignments during semester

Thursday 9 Sept
23 Sept
30 Sept
will be made up on
October Fridays
Bring schedules
GROUP THEORY

Objective: the isomorphism theorems

**Def** Let $G$ be a nonempty set equipped with a binary operation $\cdot$

$$G \times G \rightarrow G$$

$$(a,b) \mapsto ab$$

such that $\forall a,b,c$

- $(ab)c = a(bc)$
- $\exists e \in G$ such that $ae = ea = a$
- $\forall a \exists a^{-1}$ such that $aa^{-1} = a^{-1}a = e$

We say $G$ is a **GROUP** under $\cdot$, i.e. $(G, \cdot)$

**first question:** need $a^{-1}$ be unique?

Examples: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are all groups under $+$

$\mathbb{Z}/n\mathbb{Z}$ under $+$

$\mathbb{Q}\{0\}$, $\mathbb{R}\{0\}$, $\mathbb{C}\{0\}$ under $\cdot$

$GL_2(\mathbb{R})$ - general linear group size 2, i.e. \{ $(a, b) : abcde \in \mathbb{R}$ \}

under matrix multiplication with identity $(1, 0)$

with inverse

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \rightarrow \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$
Remark

If \( G \) is a group \( \ast \)
\[
ab = ba
\]
then we say \( G \) is ABELIAN and denote the operation as
\[
a \ast b = b \ast a
\]
and name the identity \( 0 \). We use the term 'ADDITIONAL ABELIAN GROUP'

to refer to this situation.

Def

Let \( G, H \) be groups under operations \( \cdot \), \( \ast \) respectively. Then \( G \times H = \{ (g, h) \mid g \in G, h \in H \} \) is a group with
\[
(g, h) \cdot (g', h') = (g \cdot g', h \ast h')
\]
is a group with identity \( (e_G, e_H) \).

Exercise: prove this.

Prop

Let \( G \) be a group

1. \( G \) has exactly one identity
2. Each \( a \in G \) has exactly one inverse
3. \( (a^{-1})^{-1} = a \)
4. \( (ab)^{-1} = b^{-1} \ast a^{-1} \)
5. \( a_1, a_2, \ldots, a_n \in G \). Then all of the products
\[
a_1 (a_2 (a_3 (\ldots (a_n \ldots))),)
\]
\[
(a_1 a_2) (a_3 (a_4 (\ldots))
\]
i.e. all parenthesizations, ordering of associations, etc., is equal
and so the product \( a_1 a_2 \ldots a_n \) is well-defined. (call this generalized associativity)

Consider 1-4 exercises, and contemplate 5.
Remarks

1. G is a group
   \( n \in \mathbb{N} \)
   Define \( a^n = \underbrace{a \cdot a \ldots a}_{n \text{ times}} \)
   \( a^{-n} = \underbrace{(a^{-1}) \ldots (a^{-1})}_{n \text{ times}} \)
   \( a^0 = e \)
   All of the usual rules for exponentiation, involving a single element, apply
   \( a^{m+n} = a^m a^n \), \( (a^m)^n = a^{mn} \)

2. Let \( G \) be an additive abelian group
   By generalized associativity, we can write
   \( a_1 + a_2 + \ldots + a_n \)
   Next, denote the inverse of an element as \(-a\)
   Denote \( a + (-b) = a - b \)
   Take for \( n \in \mathbb{N} \)
   \( na = na = \underbrace{a + a + \ldots + a}_{n \text{ times}} \)
   \((-n)a = -na = \underbrace{(-a) + \ldots + (-a)}_{n \text{ times}} \)
   \( 0 \cdot a = 0 \)
   \( \mathbb{Z} \subseteq G \)

   We can check that \( ma + na = (m+n)a \) etc

Definition

Let \( G \) be a group, \( x \in G \). If \( x^n = 1 \), for some positive integer \( n \), and \( x^m \neq 1 \) for any \( 1 \leq m < n \), then the order of \( x \) is \( n \) and we write \( |X| = n \). (And also say \( x \) has finite order). If \( x \) does not have finite order, we say \( x \) has infinite order, and write \( |X| = \infty \)

Examples

- \( \mathbb{C}^* \) (multiplicative group of nonzero complexes)
  \( e^{2\pi i/n} \) has order \( n \)
- \( \mathbb{Z} \) (under addition) every nonzero element has infinite order

N.B. \( \mathbb{R} \) not \( \neq \) addition around
Def. We refer to the cardinality of $G$ as the order of $G$ and write $|G| = n$.

$|\mathbb{Z}/n\mathbb{Z}| = n$

$|\mathbb{Z}| = \infty$

Yes, these ideas of 'the order of' are related.

§1.2 DIHEDRAL GROUPS

A symmetry of a plane geometric figure $F$ is a "rigid motion" of $F$ after which $F$ occupies the same region as before the motion.

Example. The symmetries of an equilateral triangle:

\[\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\]

\[\begin{array}{c}
\sigma_1: & 1 & \rightarrow & 2 \\
\sigma_2: & 2 & \rightarrow & 3 \\
\sigma_3: & 3 & \rightarrow & 1 \\
\end{array}\]

We may identify each symmetry with a function $[1, 2, 3] \rightarrow [1, 2, 3]$ sending vertex $i$ to position $j$.

\[\sigma_1: 1 \rightarrow 2, \quad \sigma_2: 2 \rightarrow 3, \quad \text{e.g.} \quad \sigma_2(1) = 2, \quad \sigma_2(3) = 1\]

Why are there six (6) symmetries and not some other number?

Viewing $\sigma_1, \ldots, \sigma_6$ as "operations on the triangle" we can compose symmetries:

\[\begin{array}{c}
\sigma_1 & \sigma_2 & \sigma_3 & \sigma_4 & \sigma_5 \\
1 & 2 & 3 & 2 & 1 \\
\end{array}\]

We write "algebraically" as \(\sigma_4 \circ \sigma_2 = \sigma_6\) and \(\sigma_2 \circ \sigma_4 = \sigma_5\).
We can check directly that the product is associative, or that observe that the product of symmetries corresponds to the composition of functions, which is associative.

And each symmetry has an inverse (exercise)

\[
\begin{array}{cccc}
1 & 2 & 3 & 4 & 5 \\
2 & 3 & 5 & 1 & 4 \\
3 & 1 & 5 & 4 & 2 \\
(25)(34) & (12345)
\end{array}
\]

Continuing: Set \( r = \sigma_2 \), \( s = \sigma_4 \). Can check:

\[
\begin{align*}
0_1 &= 1 = r^3 = s^2 \\
0_2 &= r \\
0_3 &= r^2 = r^{-1} \\
0_4 &= s = s^{-1} \\
0_5 &= rs = sr^2 = sr^{-1} \\
0_6 &= sr = r^2 s = r^{-1} s
\end{align*}
\]

Note: We name this group the **Dihedral Group of order six**, \( D_6 \), and we say that \( D_6 \) is generated by \( r \) and \( s \)

Moreover, the product in \( D_6 \) is defined by the relations:

\[
\begin{align*}
r^3 &= s^2 = 1 \\
rs &= sr^2 \\
rsr &= r^2
\end{align*}
\]