ek 7
dents
the same
lar -
Week 1
HW1 (1,2,3,4)
7/28/16

remark: (3) Induction also works for statements that are true for all $\mathbb{N} \ni n \geq n_0 > 1$, since $\exists$ an obvious isomorphism between $\{n_0, n_0+1, n_0+2, \dots\}$ and $\mathbb{N}$.

§2 Groups

2.1 The definition of a group

def. 1: Let $G \neq \emptyset$ be a set. Let there be a mapping $\varphi: G \times G \to G$ that assigns to every ordered pair (a,b) with $a,b \in G$ an element of G that we denote by $a \vee b$.

remark: "$\vee$" is used to denote the mapping, i.e., $\varphi(a,b) \equiv a \vee b$. It is not to be confused with the logical operator "or".

Let $\vee$ have the following properties

(i) $a \vee b \in G \quad \forall\, a,b \in G$ (closure; this is already implied by what we said above)

(ii) $(a \vee b) \vee c = a \vee (b \vee c) \equiv a \vee b \vee c$ (associativity)

(iii) $\exists\, e \in G: \quad e \vee a = a \quad \forall\, a \in G$ (existence of a neutral element e)

(iv) $a \in G \to \exists\, a^{-1} \in G: \quad a^{-1} \vee a = e$ (existence of an inverse)

Then G is called a group under the operation $\vee$, and we write $(G, \vee)$.

If, in addition,

(v) $a \vee b = b \vee a \quad \forall\, a,b \in G$

then G is called an abelian group, and $\vee$ is called commutative p10 f.p.

remark: ($\underline{1}'$) The notation $a \vee b \equiv a \cdot b \equiv ab$ and $e \equiv \underline{1}$ is used more generally, in which case the group is called "multiplicative".

remark: (1) For abelian groups, "$\vee$" is often denoted by "+" and called addition. In this case, e is usually denoted by 0 ("zero"), and a^{-1} by $-a$ ("negative a"). Instead of $a+(-a)=0$ one usually writes $a-a=0$. With these conventions, the group is called additive.

example: (1) $(\mathbb{Z},+)$, with $+$ the ordinary addition, is an abelian group with the neutral element the number zero.

(2) $(\mathbb{R},+)$ is an abelian group.

proposition 1: $\mathbb{R}\setminus\{0\}$ is an abelian group under ordinary multiplication. The neutral element is the number 1.

proof: (i) $a,b\in\mathbb{R} \rightarrow ab\in\mathbb{R}$ closure ✓

(ii) $(ab)c=a(bc)\ \forall a,b,c\in\mathbb{R}$ associativity ✓

(iii) $1a=a\ \forall a\in\mathbb{R}$ neutral element ✓

(iv) $a^{-1}=\frac{1}{a}$ exists $\forall a\in\mathbb{R}\setminus\{0\}$ and $aa^{-1}=1\ \forall a\in$ inverse ✓

(v) $ab=ba\ \forall a,b\in\mathbb{R}$

proposition 2: (a) $a\vee a^{-1}=a^{-1}\vee a=e$ (left inverse = right inverse)

and $(a^{-1})^{-1}=a$

(b) $a\vee e=e\vee a=a$ (left identity = right identity)

(c) The neutral element is unique

proof: (a) def 1 (iii), (iv) $\rightarrow a^{-1}\vee a\vee a^{-1}=e\vee a^{-1}=a^{-1}$

But a^{-1} has an inverse $(a^{-1})^{-1}$! Multiply with $(a^{-1})^{-1}$ from the left: $(a^{-1})^{-1}\vee a^{-1}\vee a\vee a^{-1}=(a^{-1})^{-1}\vee a^{-1}=e$

$$e\vee a\vee a^{-1}=a\vee a^{-1}$$

$\rightarrow$ right inverse = left inverse and $a=(a^{-1})^{-1}$.

(b) $\underline{e\vee a}=\underbrace{a\vee a^{-1}}_{=e}\vee a=\underline{a\vee e}$

(c) Suppose there were multiple neutral elements e_i $(i=1,2,\dots)$

$\rightarrow a\vee e_i=a\vee e_j=a\ \forall a$. But $a^{-1}\vee a=$ some e_i.

example: (3) The set $\{a, e\}$ with an operation $\vee$ defined by

$$e \vee e = e \,,\quad a \vee e = a \,,\quad e \vee a = a \,,\quad a \vee a = e$$

forms an abelian group.

remark: (2) For finite groups, the operation scheme can be represented as a table. For example (3) we have

	e	a
e	e	a
a	a	e

2.2 Rules of operation

Let $(G, \vee)$ be a group. Then

proposition 1: $\quad (a \vee b)^{-1} = b^{-1} \vee a^{-1} \quad \forall a, b \in G$

proof: $\quad \underline{(b^{-1} \vee a^{-1}) \vee (a \vee b)} = b^{-1} \vee a^{-1} \vee a \vee b = b^{-1} \vee e \vee b = b^{-1} \vee b = \underline{e} \qquad \square$

def. 1: (a) Let G be a multiplicative group. Then we write the composition of $n \in \mathbb{N}$ elements of G

$$a_1 \vee a_2 \vee \dots \vee a_n \equiv a_1 a_2 \dots a_n =: \prod_{\nu=1}^{n} a_\nu$$

and we define recursively $\prod_{\nu=1}^{n+1} a_\nu = \left(\prod_{\nu=1}^{n} a_\nu \right) a_{n+1}$

We call this the <u>product</u> of the <u>factors</u> $a_1, \dots, a_n$.

(b) A product of n identical factors,

$$\prod_{\nu=1}^{n} a =: a^n$$

is called the <u>n^{th} power</u> of a.

proposition 2: $\quad \prod_{\mu=1}^{m} a_\mu \prod_{\nu=m+1}^{m+n} a_\nu = \prod_{\rho=1}^{m+n} a_\rho \qquad (*)$

That is, the product of two products equals the product

proof: By induction. Let $n=1$. Then $(*)$ holds by def. 1(a).
Suppose $(*)$ holds for some value of n. Then it holds for $n+1$:

$$\prod_{\mu=1}^{m} a_\mu \prod_{\nu=1}^{n+1} a_{m+\nu} = \prod_{\mu=1}^{m} a_\mu \left(\prod_{\nu=1}^{n} a_{m+\nu} \cdot a_{m+n+1} \right)$$

$$\overset{\text{associativity}}{\Downarrow} = \left(\sum_{\mu=1}^{m} a_\mu \prod_{\nu=1}^{n} a_{m+\nu} \right) a_{m+n+1} \overset{\text{induction assumption}}{\Downarrow =} \left(\prod_{\nu=1}^{m+n} a_\nu \right) a_{m+n+1} = \prod_{\nu=1}^{m+n+1} a_\nu \qquad \square$$

corollary: (a) $a^n a^m = a^{n+m}$

Problem 8
Prove this

(b) $(a^n)^m = a^{nm}$

proof: Problem 8 4.

def. 2: The zeroth power is defined by $a^0 := e$
and negative powers by $a^{-n} := (a^{-1})^n$

remark: (1) The latter definition conforms with corollary (b)

remark: (2) For additive groups, we write

$$a_1 + a_2 + \dots + a_n =: \sum_{\nu=1}^{n} a_\nu$$

and call this the sum of the a_ν.

A sum of identical elements is a multiple of that element

$$\sum_{\nu=1}^{n} a = na$$

Prop. 2 and its corollary still hold with Π replaced by Σ, and

$$\sum_{\mu=1}^{m} a_\mu + \sum_{\nu=m+1}^{m+n} a_\nu = \sum_{\varrho=1}^{m+n} a_\varrho \qquad \text{(prop 2)}$$

• replaced by $+$:

$$na + ma = (n+m)a \qquad \text{(corollary (a))}$$

Problem 9

$$m\,na = nma \qquad \text{(corollary (b))}$$

Practice problem 10/3/..

2.3 Permutations

def. 1: Let M be a finite set, and let $P: M \to M$ be a bijective mapping. Then P is called a permutation of M.

remark: (1) If M is finite with n elements, then M has the same cardinality as $\{1, \dots, n\}$. $\to$ We can characterize any permutation P on M by its action on $\{1, \dots, n\}$:

$$P_1 = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 2 & 1 & 3 & \dots & n \end{pmatrix}, \quad P_2 = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 3 & 2 & 1 & \dots & n \end{pmatrix} \text{ etc.}$$

proposition: The set of all permutations on a finite set with n elements form a group under composition called the symmetric group S_n

proof. (i) closure ✓ by def. 1

(ii) associativity ✓ by § 1.2 prop. 1

(iii) $E = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & 2 & 3 & \dots & n \end{pmatrix}$ serves as the unit element.

(iv) Any permutation is bijective and therefore has an inverse by § 1.2 remark (3) □

remark: (2) S_n is in general not abelian, see Problem 10

Problem 10
in group S_3

2.4 Subgroups

def. 1: Let $(G, \vee)$ be a group, and let $H \subset G$ with $H \neq \emptyset$. Then H is called a subgroup of G if H is itself a group under $\vee$

remark: (1) Let $e \in G$ be the ... Then $H = \{e\}$ is a ...

Theorem 1: H is a subgroup iff $a,b \in H$ implies $a \vee b^{-1} \in H$.

proof: (1) Show that $(a,b \in H \rightsquigarrow a \vee b^{-1} \in H) \rightsquigarrow H$ is a subgroup

Suppose $a,b \in H \rightsquigarrow a \vee b^{-1} \in H$.

In particular, if $b = a \in H \rightsquigarrow a \vee a^{-1} = e \in H$

and if $a = e \rightsquigarrow e \vee b^{-1} = b^{-1} \in H$

$\rightsquigarrow$ Axioms (iii), (iv) from §2.1 are fulfilled.

Axiom (ii) is trivially fulfilled, since G and H share the associative operation $\vee$.

Now consider $a \vee b = a \vee (b^{-1})^{-1} \in H$ since $b^{-1} \in H$ if $b \in H$

$\rightsquigarrow$ Axiom (i) is fulfilled.

$\rightsquigarrow H$ is a group $\rightsquigarrow$ The condition is sufficient

B: Basic logic says $A \rightsquigarrow B$ is equivalent to not $B \rightsquigarrow$ not A

(2) Show that ($a,b \in H$ does not imply $a \vee b^{-1} \in H$) $\rightsquigarrow H$ is not a subgroup

Suppose $\exists a,b \in H : a \vee b^{-1} \notin H$.

In order for H to be a group, $b \in H$ must imply $b^{-1} \in H$.

So now we have $a, b^{-1} \in H$, but $a \vee b^{-1} \notin H$

$\rightsquigarrow$ Axiom (i) is violated $\rightsquigarrow H$ is not a group

$\rightsquigarrow$ The condition is necessary □

example: (2) Consider these two elements of S_3:

$E = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ and $P = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$. They form a subgroup g

proof: $P \circ P = E \rightsquigarrow P = P^{-1}$

$\rightsquigarrow E \circ P^{-1} = P \in g$ and $P \circ E^{-1} = P \in g$

and $E \circ E^{-1} = E \in g$ and $P \circ P^{-1} = E \in g$ □

2.5 Isomorphisms and automorphisms

def. 1: a) Let $(G, \vee)$ and $(H, *)$ be groups. Let $\varphi : G \to H$ be a bijective mapping such that, $\forall a, b \in G$, $\varphi(a \vee b) = \varphi(a) * \varphi(b)$. Then we call φ an isomorphism between G and H, say that G is isomorphic to H, and write $G \cong H$.

b) If $G = H$, and $\varphi : G \to H$ is an isomorphism, we call φ an automorphism on G.

Week 2

remark: (1) One also says that φ "respects the operation".

(probl 2 #5,6,7,8)

example: (1) Let $G = \left\{ \text{real } 2\times 2 \text{ matrices } g_\alpha \equiv \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix};\ 0 \le \alpha < 2\pi \right\}$

and $H = \left\{ \text{complex numbers } h_\beta \equiv e^{i\beta};\ 0 \le \beta < 2\pi \right\}$

Then G forms a group under matrix multiplication, and H forms a group under multiplication of complex numbers (the proofs are easy).

Now define $\varphi : G \to H$ by $\varphi(g_\alpha) = h_\alpha$. φ is clearly bijective. Furthermore,

$$g_\alpha g_\beta = \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix}\begin{pmatrix} \cos\beta & \sin\beta \\ -\sin\beta & \cos\beta \end{pmatrix} = \begin{pmatrix} \cos\alpha\cos\beta - \sin\alpha\sin\beta & \cos\alpha\sin\beta + \sin\alpha\cos\beta \\ -\sin\alpha\cos\beta - \cos\alpha\sin\beta & \cos\alpha\cos\beta - \sin\alpha\sin\beta \end{pmatrix}$$

$$= \begin{pmatrix} \cos(\alpha+\beta) & \sin(\alpha+\beta) \\ -\sin(\alpha+\beta) & \cos(\alpha+\beta) \end{pmatrix} = g_{\alpha+\beta}$$

$$\Rightarrow \varphi(g_\alpha g_\beta) = \varphi(g_{\alpha+\beta}) = h_{\alpha+\beta} = e^{i(\alpha+\beta)} = e^{i\alpha} e^{i\beta}$$

$$= h_\alpha h_\beta = \varphi(g_\alpha)\varphi(g_\beta)$$

Problem 11 ≡ [illegible]

Properties of [illegible]