Proposition Let $\sim$ be an equivalence relation on a set S. Then the set of equivalence classes form a partition of S.

Pf Let $\{S_i\}$ be the set of distinct equivalence classes of S. Then each $S_i = [x_i]$ for some $x_i \in S$.

① $S_i \neq \emptyset$ as $x_i \in [x_i] = S_i$

② $\bigcup_i S_i = \bigcup_i [x_i] = S$ because every $y \in S$ is in $[y]$.

③ $S_i \cap S_j = \emptyset$ for $i \neq j$: If $[x_i] \cap [x_j] \neq \emptyset$, then there is some $z \in [x_i] \cap [x_j]$. By what I asked you to verify previously we obtain, $[z] = [x_i]$, contradicting $[x_j]$ our choice of $\{S_i\}$.

Thus we have a partition ∎

Prop Conversely given a partition $\{S_i\}$ of a set S, we obtain an equivalence relation $\sim$ of S.

Pf Define $x \sim y \iff x, y \in S_i$ for some i.
The relevant subset U is $\bigcup_i S_i \times S_i \subseteq S \times S$ ∎

Thus, equivalence relations on S are "same as" partitions on S.

Exercises:

(0.11) List the elements in $\{a,b,c\} \times \{1,2,c\}$

(A) $\{(a,1), (a,2), (a,c), (b,1), (b,2), (b,c), (c,1), (c,2), (c,c)\}$

(0.23) Give a partition of $\mathbb{Z}$ consisting of 1 element, 2 elements, 3 elements

(A) $\{\mathbb{Z}\}$, $\{$even integers, odd integers$\}$, $\{$negative integers, $\{0\}$, positive integers$\}$

(Q) Consider a distance relation $\sim$ on $\mathbb{R}$ defined by: $x \sim y$ if and only if $|x-y| \leq 1$. Is $\sim$ an equivalence relation?

(A) No, it is not an equivalence relation. Notice that, $0 \sim 1$ and $1 \sim 2$, but $0 \not\sim 2$ ■

(0.29) Describe the partition arising from $\sim$ on $\mathbb{Z}$ given by

$$n \sim m \iff n \cdot m > 0.$$

(A) I'll leave it to you to check that this an equivalence relation. Here's a systematic way of finding the equivalence classes.

- $[0] = \{0\}$ because $n \cdot 0 = 0 \not> 0$.
- $[1] = \{1, 2, 3, 4, \dots\} = \mathbb{Z}_{>0}$, positive integers ← now try $[1]$
- $[-1] = \{-1, -2, -3, \dots\} = \mathbb{Z}_{<0}$, negative integers ← now try $[-1]$ because -1 hasn't occured yet.

We stop now as we have all elements of $\mathbb{Z}$.

//

6/20 **Groups** (Section 4)

Defn A binary relation on a set G is a function $*: G \times G \to G$. We denote $*(a,b)$ as $a*b$.

Ex $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ by $(a,b) \mapsto a+b$

Defn A group is a pair $(G,*)$ where G is a set and $*$ a binary operation such that the following hold:

① [Associativity] $\forall\, a,b,c \in G$ we have $(a*b)*c = a*(b*c)$.

② [Identity element] $\exists\, e \in G$ such that $e*a = a*e \quad \forall\, a \in G$

③ [Existence of inverses] $\forall\, a \in G$, $\exists\, b \in G$ ("a^{-1}") such that $a*b = b*a = e$.

these are called Axioms

If the context is clear we just say the group G.

Ex
- $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$
- $(\mathbb{Q}-\{0\},\times)$, $(\mathbb{R}-\{0\},\times)$, $(\mathbb{C}-\{0\},\times)$ ("$\mathbb{Q}^*$", "$\mathbb{R}^*$", "$\mathbb{C}^*$") — means remove $\{0\}$ from the set; multiplication
- $M_{m\times n}(\mathbb{R})$, the set of $m \times n$ matrices under matrix addition is a group.
- The set of functions from $\mathbb{R} \to \mathbb{R}$ is a group under function addition. $G = \{\text{functions } f: \mathbb{R} \to \mathbb{R}\}$ and given $f, g \in G$, $f*g$ corresponds to $x \mapsto f(x) + g(x)$.

So we usually denote this as $(G,+)$.

② Can you find all the identity elements and inverses in the above groups?

Non examples • $(\mathbb{Z}, \times)$ is not a group.

Pf The element 1 is an identity, but most elements don't have an inverse. For example, 3 doesn't i.e. $\nexists\, a \in \mathbb{Z}$ such that $3a = 1$.

• $(M_{n\times n}(\mathbb{R}), \times)$ is not a group under matrix multiplication.

Ex The subset of $M_{n\times n}(\mathbb{R})$ consisting of invertible matrices under multiplication is a group. This is usually called "the general linear group" and is defined by $GL_n(\mathbb{R}) = \{A \in M_{n\times n}(\mathbb{R}) : A^{-1} \text{ exists}\}$ or $\det A \neq 0$.

Pf • Closed under $\times$: If $A, B \in GL_n(\mathbb{R})$, then $A\cdot B \in GL_n(\mathbb{R})$ because $(AB)^{-1} = B^{-1}A^{-1}$ exists.

• Associativity: $\forall A, B, C \in GL_n(\mathbb{R})$, $(A\cdot B)\cdot C = A\cdot(B\cdot C)$ (order of mult. doesn't matter. Note this holds in $M_{n\times n}(\mathbb{R})$).

• Identity element: $I \in GL_n(\mathbb{R})$ and $A\cdot I = I\cdot A = A \;\forall A \in GL_n(\mathbb{R})$ "$\begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix}$" (again true in $M_{n\times n}(\mathbb{R})$).

• Inverses: If $A \in GL_n(\mathbb{R})$, then A^{-1} exists. But $(A^{-1})^{-1} = A$ exists thus $A^{-1} \in GL_n(\mathbb{R})$

Note: We could have proven everything by determinants.

Warning: Given an arbitrary group $(G, *)$ you CAN ONLY assume $*$ satisfies the three axioms on page 9.

Exercise Come up with a binary relation $*$ on $\{1,2\}$ such that $(\{1,2\}, *)$ is not a group.

Exercise How many binary relations are there on a finite set containing n elements.

What can we deduce about $(G,*)$ from the axioms?

Theorem Let $(G,*)$ be a group. Then the left, right cancellation laws hold: $\forall a,b,c \in G$ we have,

- $a*b = a*c \implies b=c$ (left cancellation)
- $b*a = c*a \implies b=c$ (right cancellation)

Pf Suppose $a*b = a*c$. Then $\exists\ a'$ such that $a'*a = e$.

$a'*(a*b) = a'*(a*c)$

$\Leftrightarrow$ [Associativity] $(a'*a)*b = (a'*a)*c$

$\Leftrightarrow$ [Assumption] $e*b = e*c$

$\Leftrightarrow$ [Identity] $b = c$

Repeat this for the other case ∎

Thm Let $(G,*)$ be a group. The identity element is unique.

Pf Let e, e' be identities. Then we have

$e*a = a*e = e$ and $e'*a = a*e' = e'$ $\forall\ a \in G$.

Taking $a = e'$ we obtain $e'*e = e$

Taking $a = e$ we obtain $e'*e = e'$.

Thus $e = e'$ ∎

Prop Let $(G,*)$ be a group. Inverses are unique.

Pf Let $a \in G$ and assume b, b' are both inverses of a. (so they satisfy axiom ③)

Then,

$$b = b*e = b*(a*b') = (b*a)*b' = e*b' = b'$$

↑ identity ↑ inverse ↑ associativity ↑ inverse ↑ identity ∎