# Linear Algebra & Geometry

LECTURE 5

Isomorphism of fields and groups

# Isomorphism

**Definition.**
Two algebras $(X, \#, *)$ and $(Y, !, ?)$ are said to be *isomorphic* iff there exists a bijection $\varphi: X \to Y$ such that for every $p, q \in X, \varphi(p \# q) = \varphi(p) ! \varphi(q)$ and $\varphi(p * q) = \varphi(p) ? \varphi(q)$. Every such bijection is called an *isomorphism* between $X$ and $Y$.

**Remark.** This definition can be easily adapted to algebras with fewer than two or more than two operations.

**Fact.**
An isomorphism preserves the "type" of the algebra. This means: if $(X, \#, *)$ and $(Y, !, ?)$ are isomorphic and one is a field then so is the other. The same for groups, Abelian groups etc.

**Outline of a proof.**
An isomorphism clearly preserves commutativity and associativity of operations. It preserves the property of "being the identity element" of an operation, in the sense that if $e$ is the identity of # then $\varphi(e)$ is the identity for !

**Fact.**
An isomorphism preserves identity elements and preserves the property of being the inverse element (of some other element).
*More precisely*:
If $e$ is the identity for an operation in $X$, then $\varphi(e)$ is the identity for the corresponding operation in $Y$.
AND
If $b$ is the inverse of $a$ in $X$, then $\varphi(b)$ is the inverse of $\varphi(a)$ (w.r.t. the corresponding operation) in $Y$.

**Proof.** Suppose $e$ is the identity of # in $X$. Consider $\varphi(e)!\, y$ for any $y \in Y$. Since $\varphi$ is a bijection there exists $x \in X$ such that $y = \varphi(x)$. Hence, $\varphi(e)!\, y = \varphi(e)!\, \varphi(x) = \varphi(e\#x) = \varphi(x) = y$.

The second part: Suppose $b$ is the inverse of $a$, i. e. $e = b\#a$. Then $\varphi(e) = \varphi(b\#a) = \varphi(b)\, !\, \varphi(a)$. We already know that $\varphi(e)$ is the identity for ! in $Y$, so $\varphi(b)$ is the inverse of $\varphi(a)$. QED

**Fact.**
The inverse function of an isomorphism $\varphi$ is itself an isomorphism.

**Proof.**
First, we should prove that the inverse function of a bijection is itself a bijection. (*This is a fact from Set Theory. I include a proof of this and other facts about bijections at the end of this presentation*).

Next, we must prove that for every $y_1, y_2 \in Y$, $\varphi^{-1}(y_1 \,!\, y_2) = \varphi^{-1}(y_1) \,\#\, \varphi^{-1}(y_2)$. Suppose $\varphi^{-1}(y_1 \,!\, y_2) \neq \varphi^{-1}(y_1) \,\#\, \varphi^{-1}(y_2)$. Since $\varphi$ is a 1-1 function applying $\varphi$ to both sides yields different values, that is, $\varphi(\varphi^{-1}(y_1 \,!\, y_2)) \neq \varphi(\varphi^{-1}(y_1) \,\#\, \varphi^{-1}(y_2))$. Obviously, on the LHS we get $\varphi\big(\varphi^{-1}(y_1 \,!\, y_2)\big) = y_1 \,!\, y_2$. Since $\varphi$ is an isomorphism, on the RHS we get $\varphi(\varphi^{-1}(y_1) \,\#\, \varphi^{-1}(y_2)) = \varphi(\varphi^{-1}(y_1)) \,!\, \varphi(\varphi^{-1}(y_2)) = y_1 \,!\, y_2$ and we obtain $y_1 \,!\, y_2 \neq y_1 \,!\, y_2$, which is a contradiction. QED

**Comprehension.**
Prove that the composition of two isomorphisms is an isomorphism too.

**Examples.**

1. Every algebra is isomorphic with itself, $\varphi = id$ can be used as an isomorphism.
2. $\varphi(z) = \overline{z}$ is an isomorphism of the field of $\mathbb{C}$ with itself which is not an identity function.
3. Look at example 6 of a field (the one with $x * y = x + y + 1$ and $x\#y = xy + x + y$). Instead of two pages of calculations we can check that $\varphi(x) = x + 1$ is an isomorphism of $(\mathbb{R}, *, \#)$ into $(\mathbb{R}, +, \cdot)$. Indeed, $\varphi(x * y) = \varphi(x + y + 1) = (x + y + 1) + 1 = x + 1 + y + 1 = \varphi(x) + \varphi(y)$ and $\varphi(x\#y) = \varphi(xy + x + y) = xy + x + y + 1 = (x + 1)(y + 1)$. Incidentally, notice that in Example 6 we found out that the identity for $*$ was $-1$ and $\varphi(-1) = 0$, which illustrates the last Fact. We also discovered that the identity for # was 0 which implies that the identity for multiplication should be 1, which it is. You can easily verify that inverses behave just as well.

4. Are fields $\left(\mathbb{Q}(\sqrt{2}), +, \cdot\right)$ and $(\mathbb{Q}, +, \cdot)$ isomorphic?
   Suppose they are and $\varphi: \mathbb{Q}\left(\sqrt{2}\right) \to \mathbb{Q}$ is an isomorphism. Then $\varphi(1) = 1$ because an isomorphism preserves identity elements and, consequently, $\varphi(2) = \varphi(1 + 1) = \varphi(1) + \varphi(1) = 2$. But we can also write $2 = \varphi(2) = \varphi\left(\sqrt{2} \cdot \sqrt{2}\right) = \varphi\left(\sqrt{2}\right)\varphi\left(\sqrt{2}\right)$ - not possible because there is no number in $\mathbb{Q}$ whose square is 2. So, the answer is NO. In a similar way one can prove that $\mathbb{R}$ and $\mathbb{C}$ (with the usual operations) are not isomorphic.
5. Group $(\mathbb{R}^+, \cdot)$ is isomorphic to $(\mathbb{R}, +)$.
   Indeed, we can use any logarithmic function as an isomorphism because they are all bijections and $\log_b pq = \log_b p + \log_b q$, no matter what you use as $b$. Notice the identity in $(\mathbb{R}^+, \cdot)$ is 1 and $\log_b 1 = 0$, which is the identity in $(\mathbb{R}, +)$. Also, for every $a > 0$ we have $\log_b a^{-1} = -\log_b a$, the inverse for $\log_b a$ in $(\mathbb{R}, +)$.

**Fact.**

If $\varphi: X \to Y$ is a bijection then $\varphi^{-1}: Y \to X$ is a bijection too.

**Proof**.

Suppose $\varphi^{-1}$ is not 1-1. Then, there exist $y_1, y_2, y_1 \neq y_2$ such that $\varphi^{-1}(y_1) = \varphi^{-1}(y_2) = x$ for some $x \in X$. But this means that $\varphi(x) = y_1$ and $\varphi(x) = y_2$, which contradicts the definition of a function.

If $\varphi^{-1}$ is not *onto* then there exists an element, say $x \in X$, such that for every $y \in Y$, $\varphi^{-1}(y) \neq x$ but this means that no value is assigned to *x* by $\varphi$ – again, this contradicts the definition of a function.

**Fact.**

If $\varphi: X \to Y$ and $\psi: Y \to Z$ are bijections, then $\psi \circ \varphi: X \to Z$ is a bijection.

**Proof.**

1. $\psi \circ \varphi$ is a 1-1 function. Suppose $(\psi \circ \varphi)(x_1) = (\psi \circ \varphi)(x_2)$. Then $\psi(\varphi(x_1)) = \psi(\varphi(x_2))$. Since $\psi$ is 1-1 we get $\varphi(x_1) = \varphi(x_2)$ and, since $\varphi$ is 1-1 we get $x_1 = x_2$.
2. $\psi \circ \varphi$ is an *onto* function. Take an element $z \in Z$. Since $\psi$ is *onto*, there exists $y \in Y$ such that $\psi(y) = z$. Since $\varphi$ is also *onto*, there exists $x \in X$ such that $\varphi(x) = y$ hence, $\psi\big(\varphi(x)\big) = z$. QED