

Elementary Group Theory



Ole Witt-Hansen

1981 (2018)

Contents

1. Algebraic structures	1
1.1 Composition	1
1.2 Logical operators.....	1
1.2 homomorphism	3
2. Groups, rings and algebras	4
2.1 Algebraic ring structures	4
2.1 Algebras (Algebraic bodies)	6
3. An extension of the rational numbers to an algebra, where the equation $x^2 = 2$ has a root..	6
3.1 The algebra of the complex numbers	9

1. Algebraic structures

The purpose of this article is to give a survey of some fundamental algebraic structure elements, namely: composition, group, rings and algebras.

These concepts are among others necessary to introduce and investigate the properties of complex (imaginary) numbers and describe the algebra of the complex numbers.

As a starting point we shall look into the properties of the integral numbers Z , the rational numbers Q , that is, integral numbers and fractions, and finally the real numbers R , which comprises the rational numbers with the irrational numbers, e.g. $\sqrt{2}$ and π

1.1 Composition

The structure of the numbers is characterized by giving two arbitrary, e.g. rational numbers one may form new numbers, written as $a + b$ or $a \cdot b$, which are also rational numbers.

We express this, as *addition* and *multiplication* are *compositions* within the set of rational numbers.

Given a set M , which may be (almost) anything, one may define a *composition* “*” (star), within the set M , which is a mapping (a function) from $M \times M$ into M .

If a, b, c belongs to M , then instead of writing $f(a, b) = c$, we shall write:

$$(1.1) \quad a * b = c$$

A composition “*” is thus a calculation rule, which to two numbers $a \in M, b \in M$ ascribe exactly one element $c \in M$, where $c = a * b$

Examples

- Addition (+) is a composition within the set of rational numbers. If a and b are rational numbers then $c = a + b$ is also a rational number.
- Multiplication (\cdot) is also a composition within the set of rational numbers: If a and b are rational numbers then $c = a \cdot b$ is a rational number as well.
- Function composition: (\circ): $h = f \circ g$ meaning $h(x) = f(g(x))$ is a composition within the set of mappings $f : R \rightarrow R$.
- The scalar product of vectors in the plane $\vec{a} \cdot \vec{b}$ is not a composition within the set of vectors, since the scalar product is a number, and not a vector.
- The cross product of vectors $\vec{a} \times \vec{b} = \vec{c}$ is on the other hand a (non commutative) composition within the set of vectors in space.
- Matrix multiplication is a (non commutative) composition within the set of e.g. 2×2 matrixes, since $\underline{C} = \underline{A} \underline{B}$ is also a 2×2 matrix.

1.2 Logical operators

In the following we shall occasionally apply some abstract mathematical notation, which allows us to formulate theorems in a compact and precise manner: These operators connects predicates (statements that are either true or false) to form new predicates.

If p and q are predicates, we thus have:

" $p \wedge q$ " reads as : " p and q ". (conjoined)
 " $p \vee q$ " reads as : " p or q " (disjunction)
 " $\neg p$ " reads as: " $\text{non } p$ ", (negation)
 " $p \Rightarrow q$ " reads as : " $\text{if } p \text{ then } q$ ", or alternatively " p implies q " (implication)
 " $p \Leftarrow q$ " reads as : " $\text{only } p \text{ if } q$ " or q implies p (inverse implication)
 " $p \Leftrightarrow q$ " read as : p " $\text{if and only if } q$ ", or alternatively p is equivalent to q " (double implication)

Using quantifiers

When you shall formulate mathematical predicates and theorems, one often uses two phrases:

"For each x applies": This is symbolically written with an *all* quatifier: $\forall x$:

"There exists an x for which it applies": Symbolically written with an *existence* quantifier : $\exists x$:

Historic note:

Until the mid 1988'ties, the use of logical operators and quantifiers were an integrated part of the 9-12 year high school curriculum in mathematics textbooks in Denmark. But after 1988 neither logical operators or quantifiers were found in the Danish textbooks, (with one exception, namely my own textbooks, which I still used until 2011). These (excellent) textbooks can be found on my home page, where they have been divided into chapters: "Elementary Mathematics 1 -11".

The advantage of using logical operators and quantifiers are evidently that you may always write predicates in the same unique, precise and short manner. The disadvantage is of course that you are obliged to learn their meaning.

A composition $*$ within a set M is said to be *commutative*, if

$$(1.2) \quad \forall a \in M \quad \forall b \in M : a * b = b * a$$

A composition $*$ within a set M is said to be *associative*, if

$$(1.3) \quad \forall a \in M \quad \forall b \in M : \forall c \in M \quad a * (b * c) = (a * b) * c$$

This may be written in the more compact form: $\forall a, b, c \in M \quad a * (b * c) = (a * b) * c$

When it concerns numbers, the commutative and associative properties are usually formulated as: The order of the addends or the factors are without importance.

An element e is said to be a *neutral element* in a composition, if and only if:

$$(1.4) \quad \forall a \in M : a * e = e * a = a$$

There can only be one neutral element: Assuming that two unequal elements e_1 and e_2 are neutral elements, then we must have:

$$e_1 * e_2 = e_2 \text{ because } e_1 \text{ is neutral and } e_1 * e_2 = e_1 \text{ because } e_2 \text{ is neutral}$$

When it comes to numbers, the neutral element for addition is 0, and the neutral element for multiplication is 1.

An element b is said to be inverse to a , if and only if

$$(1.5) \quad a * b = b * a = e$$

The inverse element to an element a is generally denoted a^{*-1} or just a^{-1} (with no misunderstanding), but other notations, as $-a$ and $\frac{1}{a}$ is also used, and not only for numbers.

If a composition is *associative* then an element may have only one inverse element.

Assuming that an element a has two inverse elements b_1 and b_2 then it applies:

$$(b_1 * a) * b_2 = e * b_2 = b_2 = b_1 * (a * b_2) = b_1 * e = b_1$$

If a has an inverse element, then the equations: $x * a = b$ and $a * x = b$ have exactly one solution.

$$x * a = b \quad \Leftrightarrow \quad x * a * a^{*-1} = b * a^{*-1} \quad \Leftrightarrow \quad x = b * a^{*-1}$$

And in the same manner

$$a * x = b \quad \Leftrightarrow \quad x = a^{*-1} * b$$

1.2 homomorphism

We shall initially consider the algebraic structure (R_+, \cdot) , that is, positive real numbers having the compositions addition and multiplication, together with the natural logarithm \ln .

The natural logarithm is a *bijection* of (R_+, \cdot) on $(R, +)$ which conserves the algebraic structure, since:

$$(1.6) \quad x = \ln(a) \quad \wedge \quad y = \ln(b) \quad \Rightarrow \quad \ln(a \cdot b) = \ln(a) + \ln(b) = x + y$$

This example motivates the definition of a **homomorphism**.

A mapping $f: (M, *)$ on (H, \circ) is called a homomorphism of $(M, *)$ on (H, \circ) . (where M and H are two sets with the compositions $*$ and \circ), if:

$$\forall a \in M \quad \forall b \in M : f(a * b) = f(a) \circ f(b)$$

If f is a bijection (as it is the case with the natural logarithm) it is called a *isomorphism*.

Let $(M, *)$ and (H, \circ) be two algebraic structures and let f be an isomorphism of $(M, *)$ on (H, \circ) , then some rather obvious theorems apply.

1. If f is an isomorphism of $(M, *)$ on (H, \circ) . Then f^{-1} is an isomorphism of (H, \circ) on $(M, *)$.

Proof:

$$\begin{aligned}
 (1.7) \quad & x = f(a) \Leftrightarrow a = f^{-1}(x) \quad \text{and} \quad y = f(b) \Leftrightarrow b = f^{-1}(y) \\
 & a * b = f^{-1}(x) * f^{-1}(y) \\
 & f(a * b) = f(a) \circ f(b) = x \circ y \Leftrightarrow f^{-1}(x \circ y) = a * b = f^{-1}(x) * f^{-1}(y)
 \end{aligned}$$

2. If $*$ is commutative/associative then \circ is also is commutative/associative.

Proof:

$$(1.8) \quad f(a * b) = f(b * a) = f(a) \circ f(b) = f(b) \circ f(a)$$

That f is associative is shown quite similar.

3. The neutral element in $(M, *)$ is mapped into the neutral element in (H, \circ) .

Proof:

$$(1.9) \quad f(a) = f(a * e_*) = f(a) \circ f(e_*) \Rightarrow f(e_*) = e_o$$

4. The inverse element in $(M, *)$ is mapped into the inverse element in (H, \circ) .

Proof:

$$f(e_*) = e_o = f(a * a^{*-1}) = f(a) \circ f(a^{*-1}) = x \circ y \Rightarrow y = x^{o^{-1}}$$

2. Groups, rings and algebras

An algebraic structure $(G, *)$ is called a group, if:

1. The composition $*$ is associative.
2. There exists a neutral element e .
3. Every element in $(G, *)$ has an inverse element.

Examples:

The set of integral numbers with the composition "plus" $(Z, +)$ forms a group.

The set of e.g. 2x2 matrices (\underline{M}, \cdot) , where $\det(\underline{M}) \neq 0$ forms a group.

Within a group the rule of shortening applies.

$$x * a = y * a \Rightarrow x = y \quad \text{and} \quad a * x = a * y \Rightarrow x = y$$

In each case it follows from "multiplying" with a^{*-1} from the left or from the right.

The last condition is, however, only necessary if the composition $*$ is not commutative.

2.1 Algebraic ring structures

Let us then assume that we have an algebraic structure, being organized by two compositions.

The composition $*$ is said to be distributive with respect to \circ , if the distributive law applies.

$$\begin{aligned}
 (2.1) \quad & \forall a, b, c \in M : a * (b \circ c) = a * b \circ a * c \\
 & \forall a, b, c \in M : (b \circ c) * a = b * a \circ c * a
 \end{aligned}$$

Example: The integral numbers Z are organized with the compositions "+" and "·", since you can multiply a parenthesis with a number using the distributive law.

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

On the other hand, "+" is not distributive with respect to "·", since the rule below is not valid in general.

$$a + (b \cdot c) = (a + b) \cdot (a + c)$$

An algebraic structure is said to make a *ring*, if:

- $(M, *)$ is a commutative group.
- \circ is commutative and associative.
- $*$ is distributive with respect to \circ , that is: $\forall a, b, c \in M : a * (b \circ c) = a * b \circ a * c$

Example: $(\mathbb{Z}, +, \cdot)$ constitutes a ring. The neutral element by addition is 0, and the neutral element by multiplication is 1. The opposite element to a by addition is written $-a$.

In the following, we shall for clarity write "+" instead of "⊕" and "·" instead of "⊙", even if the elements concerned are not numbers.

By the same token we shall write the neutral element by + as 0, and the neutral element by · as 1, even if the elements are not numbers.

The inverse element to a by + will be written as $-a$, and if there exists an inverse element with respect to · is denoted a^{-1} .

We shall then prove some minor theorems.

1. $\forall a \in M : a \cdot 0 = 0$.
2. $\forall a, b \in M : a \cdot (-b) = (-a) \cdot b = -a \cdot b$
3. $\forall a, b \in M : (-a) \cdot (-b) = a \cdot b$

Proof:

1. $a \cdot b = a \cdot (b + 0) = a \cdot b + a \cdot 0 \Rightarrow a \cdot 0 = 0$
2. $a \cdot (b + (-b)) = a \cdot 0 = 0 = a \cdot b + a \cdot (-b)$.
 $a \cdot (-b)$ is thus the inverse element to $a \cdot b$, and therefore equal to $-a \cdot b$.
3. $(-a) \cdot (-b) = -a \cdot (-b) = -(-a)b = ab$, where we have applied the result from (2).

Note that $-(-a) = a$ follows from that $-(-a)$ is the inverse element to $(-a)$ equal to a .

It is thus the universal validity of the distributive law that delivers the explanation why *plus* times *minus* gives *minus* and *minus* times *minus* gives *plus*.

If $a \neq 0 \wedge b \neq 0$ and $a \cdot b = 0$ then a and b are denoted *nil divisors*.

There exist no nil divisors within the real number system.

If a ring do not have nil divisors, the *zero rule* and the *shortening rules* apply.

The zero rule:

$$(2.2) \quad a \cdot b = 0 \Leftrightarrow a = 0 \vee b = 0$$

The shortening rule:

$$(2.3) \quad x \neq 0 \wedge x \cdot a = x \cdot b \Rightarrow a = b \text{ and accordingly: } x \neq 0 \wedge a \cdot x = b \cdot x \Rightarrow a = b$$

proof:

$$x \neq 0 \wedge x \cdot a = x \cdot b \Leftrightarrow x \cdot a - x \cdot b = 0 \Leftrightarrow x \cdot (a - b) = 0 \Leftrightarrow a - b = 0 \Leftrightarrow a = b = 0$$

2.1 Algebras (Algebraic bodies)

An algebra $(L, +, \cdot)$ is characterized as a set L , where the following conditions apply.

1. $(L, +)$ is a commutative group.
2. $(L \setminus \{0\}, \cdot)$ is a commutative group.
3. The distributive law applies: $\forall a, b, c \in M : a \cdot (b + c) = a \cdot b + a \cdot c$.

A set M is called a sub algebra of L , if $M \subseteq L$ and $(M, +, \cdot)$ constitute an algebra.

The rational numbers Q is an algebra which comprises the integral numbers Z .

The real numbers R is an algebra which has the rational numbers Q as a sub algebra.

The complex numbers C is an algebra, which has the real numbers as a sub algebra.

Two algebras $(L, +, \cdot)$ og $(M, *, \circ)$ are said to be isomorphic, if there exists a bijection φ , which meets the demands of being an isomorphism.

$$(2.3) \quad \forall a, b \in L : \varphi(a + b) = \varphi(a) * \varphi(b) \text{ and } \forall a, b \in L : \varphi(a \cdot b) = \varphi(a) \circ \varphi(b)$$

If two algebras are isomorphic, then they are algebraic identical.

You may perceive the two algebras as (algebraic) the same algebra, where just the element have changed their names from a to $\varphi(a)$, and the compositions have changed their names from "+" to "*" and from "." to "o".

At set is said to be ordered, if there exists an ordering relation "<" (comparison criteria), which meets the following claims.

1. $\forall a, b \in M : a \neq b \Rightarrow a < b \vee b < a$
2. $a < b \wedge b < c \Rightarrow a < c$ (The ordering relation is transitive)

The integral numbers Z , the rational numbers Q together with the real numbers R are ordered by the ordering relation "<", "less than".

There exists, however, no ordering relation for the complex numbers which comply with the conditions 1. and 2.

3. An extension of the rational numbers to an algebra, where the equation $x^2 = 2$ has a root

An extension of an algebra is an algebra, which has the original algebra as a sub algebra.

First we notice that no rational number can be a root in the equation $x^2 = 2$.

Assuming that a fraction $x = \frac{p}{q}$ that cannot be shortened, and where p and q are positive integers is root in the equation $x^2 = 2$, then we must have:

$$\left(\frac{p}{q}\right)^2 = 2 \Leftrightarrow p^2 = 2q^2, \text{ so that } p^2 \text{ and thus } p \text{ must be an even number.}$$

We therefore put:

$$p = 2r, \text{ and get: } \left(\frac{2r}{q}\right)^2 = 2 \Leftrightarrow 4r^2 = 2q^2 \Leftrightarrow q^2 = 2r^2$$

From which we conclude that q^2 and thereby q is an even number in contradiction to the premises that $x = \frac{p}{q}$ could not be shorten, so $x = \frac{p}{q}$ cannot be a rational number.

Let us then assume that there exists a (non rational) number x for which $x^2 = 2$, which we shall denote by $\sqrt{2}$. (The roots in $x^2 = 2$ are then $\sqrt{2}$ and $-\sqrt{2}$).

According to the reasoning above $\sqrt{2}$ can not be a rational number.

The program is then to extend the rational number to an algebra where the equation $x^2 = 2$ has a solution.

Preliminary, we do not know whether such an algebra exists, but we may establish certain demands that such an algebra must apply, to constitute an algebra.

What we are doing is called an analyze, as we assume that there actually exists an algebra, and then draw some conclusions of the properties it must have.

If $\sqrt{2}$ is actually a number, then it can be added and multiplied with rational numbers by the usual calculation rules for numbers.

From this, we conclude that if an algebra contains $\sqrt{2}$, it must also contain all numbers having the form $q_1 + \sqrt{2}q_2$, where q_1 and q_2 are arbitrary rational numbers.

By using the calculation rules for rational numbers, it turns out that the set of numbers $q_1 + \sqrt{2}q_2$ actually form an algebra. The least algebra that contains the number $\sqrt{2}$.

That the compositions "+" and "·" actually are compositions within the algebra L may be seen from the following, where p, q, r are arbitrary rational numbers.

$$(3.1) \quad \begin{aligned} (p_1 + \sqrt{2}p_2) + (q_1 + \sqrt{2}q_2) &= p_1 + q_1 + \sqrt{2}(p_2 + q_2) \\ (p_1 + \sqrt{2}p_2) \cdot (q_1 + \sqrt{2}q_2) &= p_1q_1 + 2p_2q_2 + \sqrt{2}(p_1q_2 + p_2q_1) \end{aligned}$$

From which we notice that the sum and product of two numbers are numbers belonging to L .

That the sum and product operation are both commutative, and associative is rather obvious, since the rational numbers have these properties.

Furthermore there is a zero element, namely $q_1 = q_2 = 0$, and also a one element namely: $q_1 = 1$ and $q_2 = 0$. The opposite number to $q_1 + \sqrt{2}q_2$, is obviously $-(q_1 + \sqrt{2}q_2)$.

Every element $q \in L \setminus \{0\}$ has furthermore an inverse element x , being the solution to the equation:

$$xq = 1 \Leftrightarrow x(q_1 + \sqrt{2}q_2) = 1 \Leftrightarrow$$

$$x = \frac{1}{(q_1 + \sqrt{2}q_2)} = \frac{(q_1 - \sqrt{2}q_2)}{(q_1^2 - 2q_2^2)} = \frac{q_1}{q_1^2 - 2q_2^2} - \sqrt{2} \frac{q_2}{q_1^2 - 2q_2^2}$$

From which is seen that the inverse element to q also belongs to L .

(The inverse element to $\sqrt{2}$ is $\frac{\sqrt{2}}{2}$).

You should notice that: $q_1^2 - 2q_2^2 = 0 \Rightarrow q_1 = q_2 = 0 \vee (\frac{q_1}{q_2})^2 = 2$, where the last solution is excluded, since $(\frac{q_1}{q_2})$ is a rational number.

Finally we notice that the distributive law applies; $q(r + p) = qr + qp$, where p, q, r belongs to L .

$$(q_1 + \sqrt{2}q_2)((r_1 + \sqrt{2}r_2) + (p_1 + \sqrt{2}p_2)) =$$

$$(q_1 + \sqrt{2}q_2)((r_1 + p_1) + \sqrt{2}(r_2 + p_2)) =$$

$$q_1(r_1 + p_1) + 2q_2(r_2 + p_2) + \sqrt{2}(q_2(r_1 + p_1) + q_1(r_2 + p_2)) =$$

$$q_1r_1 + 2q_2r_2 + \sqrt{2}(q_2r_1 + q_1r_2) + q_1p_1 + 2q_2p_2 + \sqrt{2}(q_2p_1 + q_1p_2) =$$

$$(q_1 + \sqrt{2}q_2)(r_1 + \sqrt{2}r_2) + (q_1 + \sqrt{2}q_2)(p_1 + \sqrt{2}p_2)$$

Notice that the validity of the distributive law is exclusively based on the established rules of calculation with rational numbers.

From this analysis, we may then establish a more formal extension of the rational numbers to an algebra, where the equation: $x^2 = 2$, has a root. Formally we proceed as follows:

We consider the set of pairs (q_1, q_2) , where q_1 and q_2 are rational numbers.

For this set we define the two compositions \oplus and \otimes in the following manner.

$$(3.2) \quad (q_1, q_2) \oplus (p_1, p_2) = (q_1 + p_1, q_2 + p_2)$$

$$(q_1, q_2) \otimes (p_1, p_2) = (q_1p_1 + 2q_2p_2, p_1q_2 + q_2p_1)$$

According to the analysis, we have already made, it is obvious that the set.

$$L = \{(q_1, q_2) \mid q_1 \in \mathbb{Q} \wedge q_2 \in \mathbb{Q}\}$$

With the compositions defined above forms an algebra.

It should also be clear (and it can easily be verified) that the set:

$$Q_1 = \{(q_1, 0) \mid q_1 \in Q\}$$

Is isomorphic with the set of rational numbers.

Clearly the zero-element in L is $(0,0)$ and the one-element in L is $(1,0)$.

As an example, we shall show that $\left(\frac{q_1}{q_1^2 - 2q_2^2}, -\frac{q_2}{q_1^2 - 2q_2^2}\right)$ is the inverse element to (q_1, q_2) .

$$\begin{aligned} (q_1, q_2) \otimes \left(\frac{q_1}{q_1^2 - 2q_2^2}, -\frac{q_2}{q_1^2 - 2q_2^2}\right) &= \\ \left(q_1 \frac{q_1}{q_1^2 - 2q_2^2} - 2q_2 \frac{q_2}{q_1^2 - 2q_2^2}, q_2 \frac{q_1}{q_1^2 - 2q_2^2} - q_1 \frac{q_2}{q_1^2 - 2q_2^2}\right) &= (1, 0) \end{aligned}$$

Finally we may calculate: $(0,1) \otimes (0,1) = (2,0)$

If we denote $(0,1)$ by the symbol $\sqrt{2}$ and identify $(2,0)$ with the rational number 2 (caused by the mentioned isomorphism), clearly: $(0,1) = \sqrt{2} \in L$ and $(\sqrt{2})^2 = 2$.

What we have formally accomplished is to extend the rational numbers to an algebra where the equation:

$$x^2 = 2 \quad \text{has a root.}$$

3.1 The algebra of the complex numbers

Following the same guidelines as above, we are now able to show that we may extend the real numbers to an algebra, where the equation.

$$x^2 = -1 \quad \text{has a root.}$$

This algebra is, as you know, called the complex (or imaginary) numbers, and the two roots in the equation $x^2 = -1$ are denoted i and $-i$, where we have $i^2 = -1$.

Analogous to the previous extension of the rational numbers, we write a complex number

$$(a_1, a_2) = a_1 + ia_2 \quad \text{instead of} \quad (q_1, q_2) = q_1 + \sqrt{2}q_2$$

From an algebraic point of view, there is no structural difference in the two extensions we have made.

If we carefree make algebraic operations with complex numbers, as it was real numbers, remembering that $i^2 = -1$ we get the following compositions for addition and multiplication:

$$(3.5) \quad \begin{aligned} a + b &= a_1 + ia_2 + (b_1 + ib_2) = a_1 + b_1 + i(a_2 + b_2) \\ a - b &= a_1 + ia_2 - (b_1 + ib_2) = a_1 - b_1 + i(a_2 - b_2) \end{aligned}$$

$$(3.6) \quad a \cdot b = (a_1 + ia_2) \cdot (b_1 + ib_2) = a_1b_1 - a_2b_2 + i(a_2b_1 + a_1b_2)$$

You may easily convince yourself that the complex numbers as defined with these compositions constitutes an algebra.

That the compositions are commutative are evident, and the associative and distributive law can be shown as in the previous example of an extension of an algebra.

That the real numbers 0 and 1 are the neutral elements by addition and multiplication follows immediately from (3.5) and (3.6).

To demonstrate that every complex number different from zero has an inverse element is most easily accomplished by introducing the complex conjugate number \bar{a} to any complex number $a = (a_1 + ia_2)$.

$$(3.7) \quad \bar{a} = a_1 - ia_2$$

Then it follows:

$$(3.7) \quad a \cdot \bar{a} = |a|^2 = (a_1 + ia_2)(a_1 - ia_2) = a_1^2 + a_2^2$$

where

$$(3.8) \quad |a| = \sqrt{a_1^2 + a_2^2}$$

Is called the modulus (or the numeric value) of a complex number.

To determine the inverse number to a complex number $a + ib$, we must find a complex number $x + iy$, such that:

$$(a + ib)(x + iy) = 1$$

Multiplying this equation by $a - ib$, the complex conjugate to $a + ib$, we get:

$$(3.9) \quad (a^2 + b^2)(x + iy) = a - ib \Rightarrow x + iy = \frac{a - ib}{(a^2 + b^2)}$$

There is a tradition for not writing an imaginary number in the denominator of a fraction, so if we must evaluate $\frac{a}{b}$, where $a = (a_1 + ia_2)$ and $b = (b_1 + ib_2)$ are complex numbers, we simply

multiply by the complex conjugate number to b in the numerator and denominator:

$$(3.10) \quad \frac{a}{b} = \frac{a\bar{b}}{b\bar{b}} = \frac{a\bar{b}}{|b|^2} = \frac{(a_1 + ia_2)(b_1 - ib_2)}{b_1^2 + b_2^2}$$

The complex numbers are treated more extensively in the paper "Complex numbers" in my home page under mathematics.