MATH 415

Modern Algebra I

Lecture 24: Quaternions. Field of quotients.

Complex numbers as an $\mathbb{R}$-algebra

Complex numbers can be defined as a certain 2-dimensional algebra over the field $\mathbb{R}$. We have a distinguished basis $\mathbf{1}, i$. Hence every complex number z is uniquely represented as $z = x\mathbf{1} + yi$, where $x, y \in \mathbb{R}$.

Since multiplication is a bilinear function, it is enough to define $z_1 \cdot z_2$ in the case $z_1, z_2 \in \{\mathbf{1}, i\}$. We set $\mathbf{1} \cdot \mathbf{1} = \mathbf{1}$, $\mathbf{1} \cdot i = i \cdot \mathbf{1} = i$ and $i \cdot i = -\mathbf{1}$.

Because of bilinearity of the product, it is easy to check that $\mathbf{1} \cdot z = z \cdot \mathbf{1}$, $z_1 \cdot z_2 = z_2 \cdot z_1$ and $(z_1 \cdot z_2) \cdot z_3 = z_1 \cdot (z_2 \cdot z_3)$.

Quaternions

The **Hamilton quaternions** $\mathbb{H}$ can be defined as a certain 4-dimensional algebra over the field $\mathbb{R}$. We have a distinguished basis $\mathbf{1}, i, j, k$. Hence every quaternion q is uniquely represented as $z = a\mathbf{1} + bi + cj + dk$, where $a, b, c, d \in \mathbb{R}$.

Since multiplication is a bilinear function, it is enough to define $q_1 \cdot q_2$ for $q_1, q_2 \in \{\mathbf{1}, i, j, k\}$. We set $\mathbf{1} \cdot \mathbf{1} = \mathbf{1}$, $\mathbf{1} \cdot i = i \cdot \mathbf{1} = i$, $\mathbf{1} \cdot j = j \cdot \mathbf{1} = j$, $\mathbf{1} \cdot k = k \cdot \mathbf{1} = k$, $i \cdot i = j \cdot j = k \cdot k = -\mathbf{1}$, $i \cdot j = k$, $j \cdot i = -k$, $j \cdot k = i$, $k \cdot j = -i$, $k \cdot i = j$, $i \cdot k = -j$.

Theorem $\mathbb{H}$ is a non-commutative division ring.

Lemma 1 $q \cdot \mathbf{1} = \mathbf{1} \cdot q = q$ for all $q \in \mathbb{H}$.

Proof. Since $f_1(q) = q \cdot \mathbf{1}$, $f_2(q) = \mathbf{1} \cdot q$ and $f_3(q) = q$ are all linear functions on $\mathbb{H}$, it is enough to prove the equalities in the case when $q \in \{\mathbf{1}, i, j, k\}$. In this case they follow from the definition of multiplication.

Lemma 2 For any $a, b \in \mathbb{R}$ and $q \in \mathbb{H}$ we have $(a\mathbf{1}) + (b\mathbf{1}) = (a + b)\mathbf{1}$, $(a\mathbf{1}) \cdot (b\mathbf{1}) = (ab)\mathbf{1}$ and $(a\mathbf{1}) \cdot q = aq$.

In view of Lemma 2, we can identify any quaternion of the form $a\mathbf{1}$ with the real number a so that $\mathbb{R} \subset \mathbb{H}$. This also allows to consider scalar multiplication on $\mathbb{H}$ as a special case of multiplication of quaternions. In particular, we can use the same notation $q_1 q_2$ for both kinds of multiplication.

Lemma 3 Multiplication of quaternions is associative.

Idea of the proof. Since $(q_1q_2)q_3$ and $q_1(q_2q_3)$ are both trilinear functions of $q_1, q_2, q_3 \in \mathbb{H}$, it is enough to prove the equality $(q_1q_2)q_3 = q_1(q_2q_3)$ in the case when $q_1, q_2, q_3 \in \{\mathbf{1}, i, j, k\}$.

For any quaternion $q = a + bi + cj + dk$, we define the **conjugate** quaternion by $\bar{q} = a - bi - cj - dk$ and the **modulus** of q by $|q| = \sqrt{a^2 + b^2 + c^2 + d^2}$.

Lemma 4 $q\bar{q} = \bar{q}q = |q|^2$ for all $q \in \mathbb{H}$.

Lemma 5 Every nonzero quaternion q has a multiplicative inverse: $q^{-1} = |q|^{-2}\bar{q}$.

Rational quaternions are quaternions of the form $q = a + bi + cj + dk$, where $a, b, c, d \in \mathbb{Q}$. The rational quaternions also form a division ring.

Integer quaternions are quaternions of the form $q = a + bi + cj + dk$, where $a, b, c, d \in \mathbb{Z}$. The integer quaternions form a ring. This ring has only 8 invertible elements (the units): $\pm 1, \pm i, \pm j, \pm k$. These 8 elements form a group under quaternion multiplication, called **the quaternion group** and denoted Q_8.

Theorem Any non-abelian group of order 8 is isomorphic either to the dihedral group D_4 or to the quaternion group Q_8.

From a ring to a field

Question 1. When a ring R can be extended to a field?

An obvious necessary condition is commutativity. Another necessary condition is absence of zero divisors (which is equivalent to cancellation laws).

Proposition If an element of a ring with unity has a multiplicative inverse, then it is not a divisor of zero.

Question 2. When a semigroup S can be extended to a group?

Theorem If S is a commutative semigroup with cancellation, then it can be extended to an abelian group G. Moreover, if $G = \langle S \rangle$, then any element of G is of the form $b^{-1}a$, where $a, b \in S$. Moreover, if $G = \langle S \rangle$, then the group G is unique up to isomorphism.

Theorem Any finite semigroup with cancellation is actually a group.

Lemma If S is a finite semigroup with cancellation, then for any $s \in S$ there exists an integer $k \geq 2$ such that $s^k = s$.

Proof: Since S is finite, the sequence $s, s^2, s^3, \ldots$ contains repetitions, i.e., $s^k = s^m$ for some $k > m \geq 1$. If $m = 1$ then we are done. If $m > 1$ then $s^{m-1}s^{k-m+1} = s^{m-1}s$, which implies $s^{k-m+1} = s$.

Proof of the theorem: Take any $s \in S$. By Lemma, we have $s^k = s$ for some $k \geq 2$. Then $e = s^{k-1}$ is the identity element. Indeed, for any $g \in S$ we have $s^k g = sg$ or, equivalently, $s(eg) = sg$. After cancellation, $eg = g$. Similarly, $ge = g$ for all $g \in S$. Finally, for any $g \in S$ there is $n \geq 2$ such that $g^n = g = ge$. Then $g^{n-1} = e$, which implies that $g^{n-2} = g^{-1}$.

Field of quotients

Theorem A ring R with unity can be extended to a field if and only if it is an integral domain.

If R is an integral domain, then there is a (smallest) field F containing R called the **quotient field** of R (or the **field of quotients**). Any element of F is of the form $b^{-1}a$, where $a, b \in R$. The field F is unique up to isomorphism.

Examples. • The quotient field of $\mathbb{Z}$ is $\mathbb{Q}$.
• The quotient field of $\mathbb{R}[X]$ is $\mathbb{R}(X)$.
• The quotient field of $\mathbb{Z}[\sqrt{2}] = \{m + n\sqrt{2} \mid m, n \in \mathbb{Z}\}$ is $\mathbb{Q}[\sqrt{2}] = \{p + q\sqrt{2} \mid p, q \in \mathbb{Q}\}$.