LECTURE 9

Integers, Rational Numbers, and Algebraic Numbers

In the set $\mathbb{N}$ of natural numbers only the operations of addition and multiplication can be defined. For allowing the operations of subtraction and division quickly take us out of the set $\mathbb{N}$;

$$2 \in \mathbb{N} \text{ and} 3 \in \mathbb{N} \quad \text{but} 2 - 3 = -1 \notin \mathbb{N}$$

$$1 \in \mathbb{N} \text{ and} 2 \in \mathbb{N} \quad \text{but} 1 \div 2 = \frac{1}{2} \neq \mathbb{N}$$

The set $\mathbb{Z}$ of *integers* is formed by expanding $\mathbb{N}$ to obtain a set that is closed under subtraction as well as addition.

$$\mathbb{Z} = \{0, -1, +1, -2, +2, -3, +3, \dots\} \quad .$$

The new set $\mathbb{Z}$ is not closed under division, however. One therefore expands $\mathbb{Z}$ to include fractions as well and arrives at the number field $\mathbb{Q}$, the *rational numbers*. More formally, the set $\mathbb{Q}$ of rational numbers is the set of all ratios of integers:

$$\mathbb{Q} = \left\{ \frac{p}{q} \mid p, q \in \mathbb{Z} \ , \ q \neq 0 \right\}$$

The rational numbers appear to be a very satisfactory algebraic system until one begins to tries to solve equations like

$$x^2 = 2 \quad .$$

It turns out that there is no rational number that satisfies this equation. To see this, suppose there exists integers p, q such that

$$2 = \left(\frac{p}{q} \right)^2 \quad .$$

We can without loss of generality assume that p and q have no common divisors (i.e., that the fraction $\frac{p}{q}$ is reduced as far as possible). We have

$$2q^2 = p^2$$

so p^2 is even. Hence p is even. Therefore, p is of the form $p = 2k$ for some $k \in \mathbb{Z}$. But then

$$2q^2 = 4k^2$$

or

$$q^2 = 2k^2$$

so q is even, so p and q have a common divisor - a contradiction since p and q are can be assumed to be relatively prime. Thus, no such p and q exist. ∎

Yet $\sqrt{2}$ certainly exists; at the very least one can represent the number $\sqrt{2}$ geometrically as the diagonal length of a square whose sides have unit length. To handle such numbers we must widen our number field even further.

DEFINITION 9.1. *A number is called an* ***algebraic number*** *if if satisfies a polynomial equation*

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0 \tag{9.1}$$

where the coefficients $a_n, a_{n-1}, \dots, a_0$ *are all integers,* $a_n \neq 0$*, and* $n > 0$*.*

We note that rational numbers are always algebraic numbers since a rational number $\frac{p}{q}$ is a solution of

$$qx + (-p) = 0 \quad .$$

On the other hand, not every real number is algebraic. Certain numbers like π or e are known not to satisfy any algebraic equation like (2.1). Numbers which can not be represented as the solutions of equations like (2.1) are called **transcendental.** It is in general a very difficult problem to decide whether a given number is transcendental or algebraic. e, π, e^π, and $\sqrt{2}^{\sqrt{2}}$ are all transcendental. The last case, however, was not proved until 1934. It is unknown whether π^π, $e\pi$, or $e + \pi$ are algebraic or transcendental.

However, we do have a test to decide whether an algebraic number is rational or not.

THEOREM 9.2. *(Rational Zeros Theorem) Suppose that $a_n, a_{n-1}, \ldots, a_0$ are integers and that r is a rational number satisfying the polynomial equation*

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0$$

where $n \geq 1$, $a_n \neq 0$ and $a_0 \neq 0$. Write $r = \frac{p}{q}$ where p and q are integers such that $q \neq 0$ and having no common factors except ± 1. Then q divides a_n and p divides a_0.

Proof. We first recall the Fundamental Theorem of Arithmetic which states that every integer n has a factorization

$$n = (p_1)^{a_1} (p_2)^{a_2} \cdots (p_k)^{a_k}$$

where the $\{p_i\}$ are distinct prime numbers and that this factorization is unique up to the ordering of factors and the sign of pairs of factors.

Suppose that $r = \frac{p}{q}$ has the stated properties. So

$$a_n \left(\frac{p}{q}\right)^n + a_{n-1} \left(\frac{p}{q}\right)^{n-1} + \cdots + a_1 \left(\frac{p}{q}\right) + a_0 = 0 \quad .$$

Multiplying both sides by q^n yields

$$a_n p^n + a_{n-1} q p^{n-1} + \cdots a_1 p q^{n-1} + a_0 q = 0 \quad , \tag{9.2}$$

or

$$a_0 q^n = p \left(-a_n p^{n-1} - a_{n-1} q p^{n-2} - \cdots - a_1 q^{n-1}\right) \quad .$$

Hence, p divides $a_o q^n$. Since p and q are assumed to have no common factors, p must divide a_o.

Alternatively, we can also rewrite (2.2) as

$$a_n p = q \left(-a_{n-1} p^{n-1} - \cdots - a_1 p q^{n-2} - a_0 q^{n-1}\right)$$

and so q divides $a_n p$. Since p and q are assumed to have no common factors, q must divide a_n. ∎

Example: Show that the solution of $x^2 - 6$ is irrational.

According to the theorem above, if $\frac{p}{q}$ is a solution of $x^2 - 6 = 0$ then p must divide 6 and q must divide 1. Thus, the only possible rational solutions are

$$x = \pm 1, \pm 2, \pm 3, \pm 6 \quad .$$

But then

$$x^2 = 1, 4, 9, 36 \neq 6 \quad .$$

So no rational solution exists.

3. Fields and Ordered Fields

The rational numbers $\mathbb{Q}$ and the real numbers $\mathbb{R}$ are examples of what is called an *ordered field*. More generally, a *field* is a set F upon which operations of "addition" and "multiplication" are defined and for which the following axioms are satisfied:

A1. $a+(b+c)=(a+b)+c$ for all $a,b,c\in F$.
A2. $a+b=b+a$ for all $a,b\in F$.
A3. There exists $0\in F$ such that $a+0=a$ for all $a\in F$.
A4. For each $a\in F$ there is an element $-a\in F$ such that $a+(-a)=0$.
M1. $a(bc)=(ab)c$ for all $a,b,c\in F$.
M2. $ab=ba$ for all $a,b\in F$.
M3. There exists $1\in F$ such that $a\cdot 1=a$ for all $a\in F$.
M4. For each $a\in F$, there exists $a^{-1}\in F$ such that $aa^{-1}=1$.
DL. $a(b+c)=ab+bc$ for all $a,b,c\in F$.

THEOREM 9.3. *Suppose F is a field. Then if $a,b,c\in F$*

(i) $a+c=b+c$ *implies* $a=b$.
ii) $a\cdot 0=0$ *for all* $a\in F$.
(iii) $(-a)b=-(ab)$ *for all* $a,b\in F$.
(iv) $(-a)(-b)=ab$ *for all* $a,b\in F$.
(v) $ac=bc$ *and* $c\neq 0$ *implies* $a=b$.
(vi) $ab=0$ *implies either* $a=0$ *or* $b=0$.

An *ordered field* is a field F with the an order relation $\preceq$ satisfying the following axioms:

O1. Given $a,b\in F$, then either $a\preceq b$ or $b\preceq a$.
O2. If $a\preceq b$ and $b\preceq a$, then $a=b$.
O3. If $a\preceq b$ and $b\preceq c$, then $a\preceq c$.
O4. If $a\preceq b$, then $a+c\preceq b+c$.
O5. If $a\preceq b$ and $0\preceq c$, then $ac\preceq bc$.

In the theorem below we use the notation $a\prec b$ to mean $a\preceq b$ and $a\neq b$.

THEOREM 9.4. *If F is an ordered field is an ordered field and $a,b,c\in F$, then:*

(i) *If* $a\preceq b$, *then* $-b\preceq -a$.
(ii) *If* $a\preceq b$ *and* $c\preceq 0$, *then* $bc\preceq ac$.
(iii) *If* $0\preceq a$ *and* $0\preceq b$, *then* $0\preceq ab$.
(iv) $0\preceq a^2$ *for all* $a\in F$.
(v) $0\prec 1$.
(vi) *if* $0\prec a$, *then* $0\prec a^{-1}$.
(vii) *if* $0\prec a\prec b$, *then* $0\prec b^{-1}\prec a^{-1}$.

Taking $F=\mathbb{Q}$ and $\preceq$ to coincide with the the usual numerical inequality $\leq$, the above properties should seem quite elementary. However, in our context (the *axiomatic development* of number fields) these statements are properties which must first be proved before they can be employed. This we shall do next time.