M7210 Lecture 26 Monday October 22, 2012

Commutative Rings I

Reminder:

Definition. A *ring* is an abelian group A (with operations $+$, $-$ and 0) equipped with a multiplication $A \times A \to A; (a, b) \mapsto a\,b$ that satisfies the following axioms:
a) The multiplication is associative, i.e., for all $a, b, c \in A$, $(ab)c = a(bc)$.
b) The multiplication distributes over addition, i.e., for all $a, b, c \in A$, $a(b+c) = ab+ac$ and $(b+c)a = ba + ca$.
c) The multiplication has an identity, i.e., there is $1_A \in A$ such that $1_A a = a 1_A$ for all $a \in A$.[1]

A function $\phi : A \to B$ between rings is a *ring homomorphism* if it preserves addition, multiplication and identity: $\phi(a + a') = \phi(a) + \phi(a')$, $\phi(a\,a') = \phi(a)\,\phi(a')$, $\phi(1_A) = 1_B$.

A is said to be *commutative* if $ab = ba$ for all $a, b \in A$. *In this lecture, all rings will be commutative.*

Examples of commutative rings.

1. Old friends. Commutative rings that have already appeared in this course include $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$. For any integer n, $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring (with addition and multiplication are both understood "mod n").

2. Polynomial rings. If A is a commutative ring, then the ring of *polynomials with coefficients from* A is the set of all sequences $b : \mathbb{N} \to A$ that are non-zero for finitely many $i \in \mathbb{N} = \{0, 1, 2, \ldots\}$. Such sequences are called *polynomials*. Addition is defined by $(b + c)_i = b_i + c_i$. Multiplication is defined by $(bc)_i = \sum_{j+k=i} b_j c_k$. The element of this ring that is zero at all $i \in \mathbb{N}$ except $i = 1$, where its value is 1_A, is often called the *variable* or the *indeterminate*. When we say, "Let $A[x]$ be the ring of polynomials with indeterminate x," we mean that the symbol "x" is to be used as a name for this element. $A[x]$ contains a copy of A, namely, the sequences c such that $c_i = 0$ for all i except $i = 0$.[2,3]

---

[1] Sometimes rings without identity are considered, but in these lectures, we will always assume identity.

[2] A polynomial ring is a particular kind of *monoid ring*. A *monoid* is a set equipped with an associative operation that has an identity. If M is a commutative monoid and A is a commutative ring, then $A[M]$ denotes the set of all functions $b : M \to A$ that are non-zero for finitely many $m \in M$. Addition and multiplication are defined as for polynomials: assuming the operation of M is denoted $*$, we let

$$(ab)_m = \sum \{\, a_k b_\ell \mid k, \ell \in M \,\&\, k * \ell = m \,\}.$$

[3] Another generalization of the polynomials is the *ring of formal power series* with coefficients from A. This is defined just as the polynomial ring except that the condition that the sequences be non-zero for finitely many $i \in \mathbb{N}$ is dropped. Multiplication still makes sense because for any $i \in \mathbb{N}$, there are only finitely many pairs $(j, k) \in \mathbb{N}^2$ such that $j + k = i$.

3. Algebraic and Transcendental Numbers. Let θ be a complex number. $\mathbb{Q}[\theta]$ denotes the smallest subring of $\mathbb{C}$ that contains $\mathbb{Q}$ and θ. If the powers $\{1, \theta, \theta^2, \ldots\}$ are *not* linearly independent over $\mathbb{Q}$, we say that θ is an *algebraic number*. If the powers of θ *are* linearly independent over $\mathbb{Q}$, then we say that θ is *transcendental*. In this case, $\mathbb{Q}[\theta]$ is isomorphic to the polynomial ring $\mathbb{Q}[x]$.

There are only countably many algebraic numbers because there are only countably many polynomials with coefficients from $\mathbb{Q}$ and each has only finitely many roots. Therefore, the set of algebraic numbers has measure zero. With probability 1, a randomly chosen complex number is transcendental.

3.a. Algebraic Number Fields. We will show:

Proposition. *If θ is an algebraic number, then: a) $\mathbb{Q}[\theta]$ is finite-dimensional as a $\mathbb{Q}$-vector space, and b) $\mathbb{Q}[\theta]$ is a field.*

Proof of a). Let n is the least integer such that $\{1, \theta, \theta^2, \ldots, \theta^n\}$ is not independent over $\mathbb{Q}$. Then θ satisfies a polynomial equation with coefficients in $\mathbb{Q}$ of the following form:

$$0 = p(\theta) = c_0 + c_1\theta + \cdots + c_n\theta^n,\ c_0 \neq 0, c_n \neq 0. \tag{1}$$

Thus, θ^n can be expressed as a $\mathbb{Q}$-linear combination of $1, \theta, \ldots, \theta^{n-1}$. It follows (by induction) that any positive power of θ can be expressed in manner.[5] Thus, the Q-vector space spanned by $1, \theta, \ldots, \theta^{n-1}$ is closed under multiplication.

We will continue with the proof of part b) next time.

[5] Suppose that every power of θ up to the $(n+k)^{th}$ is a $\mathbb{Q}$-linear combination of $1, \theta, \ldots, \theta^{n-1}$. To see that θ^{n+k+1} is also so expressible, multiply equation (1) by θ^{k+1}. This shows that θ^{n+k+1} can be expressed as a Q-linear combination of lower powers, but each of these is a $\mathbb{Q}$-linear combination of $1, \theta, \ldots, \theta^{n-1}$.