M7210 Lecture 27 Monday October 22, 2012

Commutative Rings: Examples from number theory (cont.)

3.a. Algebraic Number Fields.

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). Proved last time

Proof of b). Suppose that $\alpha \in \mathbb{Q}[\theta] \setminus \{0\}$. Since $\mathbb{Q}[\theta]$ has $\mathbb{Q}$-dimension n, $\{1, \alpha, \alpha^2, \ldots \alpha^n\}$ satisfy a $\mathbb{Q}$-linear relation, say:

$$0 = c_j\alpha^j + c_{j+1}\alpha^{j+1} + \cdots c_k\alpha^k,\ 0 \le j < k \le n,\ c_j, \ldots, c_k \in \mathbb{Q},\ c_j \neq 0,\ c_k \neq 0.$$

We can cancel α^j and divide by c_j to get:

$$0 = 1 + \frac{c_{j+1}}{c_j}\alpha + \frac{c_{j+2}}{c_j}\alpha^2 + \cdots + \frac{c_k}{c_j}\alpha^{k-j}.$$

Thus,

$$1 = \alpha\left(\frac{-c_{j+1}}{c_j} + \frac{-c_{j+2}}{c_j}\alpha + \cdots + \frac{-c_k}{c_j}\alpha^{k-j-1}\right).$$

3.b. Algebraic Integers. Suppose $x \in \mathbb{C}$. We say that x is an *algebraic integer* if x satisfies polynomial equation of the form

$$0 = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0,\ a_{n-1}, \ldots, a_0 \in \mathbb{Z}.$$

We are requiring that the coefficient of the highest degree term be 1—such a polynomial is said to be *monic*. We are also requiring that all other coefficients be in $\mathbb{Z}$. Examples of algebraic integers are i (a root of X^2+1), $\sqrt{2}$ (a root of X^2-2), $\frac{-1+i\sqrt{3}}{2}$ (a root of X^3-1) and any n^{th} root of unity (roots of $X^n - 1 = 0$). A complex number of the form $a + b\,i$, $a, b \in \mathbb{Z}$ is called a Gaussian integer. Every Gaussian integer is an algebraic integer because $a + b\,i$ is a root of $X^2 - 2aX + a^2 + b^2$.

Proposition. *The algebraic integers form a subring of $\mathbb{C}$.*

Proof. (See Knapp, page 340.) We need to show that sums and products of algebraic integers are algebraic integers. Suppose x and y are algebraic integers satisfying equations $0 = x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0$ and $0 = y^n + b_{n-1}y^{n-1} + \cdots + b_1y + b_0$. Let $M \subset \mathbb{C}$ be the $\mathbb{Z}$-module generated by all products x^iy^j with $0 \le i < m$ and $0 \le j < n$. Then by virtue of the monic equations that x and y satisfy, $xM \subseteq M$ and $yM \subseteq M$, so $(x \pm y)M \subseteq M$ and $xyM \subseteq M$. The desired result then follows from

Lemma. *Suppose A is a finitely-generated (additive) subgroup of $\mathbb{C}$, and suppose $z \in \mathbb{C}$. If $zA \subseteq A$, then z is an algebraic integer.*

Proof. A is finitely generated and torsion-free, so it is a free $\mathbb{Z}$-module. Let $z_1, \ldots, z_r$ be a basis. Since $zz_i \in A$, the are unique integers c_{ij} such that

$$zz_i = \sum_{j=1}^{n} c_{ij}z_j,\ i = 1, \ldots, n.$$

This equation says that z is an eigenvalue for the matrix $C = \{c_{ij}\}$ with eigenvector $\begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix}$.

Thus $\det(zI - C) = 0$. Now $\det(zI - C) = 0$ is monic as a polynomial in z. The entries in C are integers, so $\det(zI - C)$ has integer coefficients. Thus, z is an algebraic integer. /////

Let $\mathcal{O}$ denote the ring of algebraic integers. If $\mathbb{Q}[\theta]$ is an algebraic number field, then its ring of integers is $\mathcal{O} \cap \mathbb{Q}[\theta]$.

Fact. $\mathcal{O} \cap \mathbb{Q} = \mathbb{Z}$. *Proof.* Any rational number may be expressed as p/q with p and q integers, $q > 0$ and $(p, q) = 1$. Pick any rational number in $\mathcal{O}$ and write it this way. Then $0 = (p/q)^n + a_{n-1}(p/q)^{n-1} + \cdots + a_0$ for some $a_i \in \mathbb{Z}$. Multiply by q^n to obtain $0 = p^n + a_{n-1}p^{n-1}q + \cdots + a_0 q^n$. This shows that p^n is a multiple of q, and since $(p, q) = 1$ this implied that $q = 1$.

Homework.

In preparation for material coming soon (Friday or next Monday), **look up** the definitions of: "irreducible element", "prime element", "unique factorization domain", "principal ideal domain".

The following are due Monday, October 29.

Exercise. Show that $A[x]$ has the following universal mapping property. If T is any (commutative) ring, $t_0 \in T$ is any element and $\phi : A \to T$ is any ring homomorphism, then there is a unique ring homomorphism $\overline{\phi} : A[x] \to T$ that agrees with ϕ on A and satisfies $\overline{\phi}(x) = t_0$.

Exercise. Show that $\mathcal{O} \cap \mathbb{Q}[i] = \mathbb{Z}[i]$. ($\mathbb{Z}[i]$ is called the *ring of Gaussian integers*.) Hint. You may use the fact that if $a + bi$, $a, b \in \mathbb{R}$ is a root of a polynomial with real coefficients, the $a - bi$ is also a root.

Exercise. Knapp, page 440, Problem 8.

Challenge. What is $\mathcal{O} \cap \mathbb{Q}[\sqrt{-3}]$? (Hint: It is not $\mathbb{Z}[\sqrt{-3}]$; there are more elements.)