Algebraic Numbers, Algebraic Integers

September 27, 2012

1 Homework set due October 4

1. Page 77; Exercises 4-7, 17,18
2. Page 78 Exercise 23
3. Page 86 Exercise 1.

2 Algebraic integers; rings of algebraic integers

Definition 1 *An algebraic integer is a root of a monic polynomial with rational integer coefficients.*

Proposition 1 *A rational number that is an algebraic integer is a good old-fashioned integer.*

Proof: Let $f(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in \mathbf{Z}[X]$ be a polynomial having the rational number r as a root. Write $r = b/d$ in lowest terms (so $gcd(b,d) = 1$) and note then that we have:

$$b^n + db^{n-1}a_{n-1} + d^2b^{n-2}a_{n-1} + \ldots + d^n a_0 = 0.$$

Reduce this modulo d to get $b^n \equiv 0$ modulo d. Conclude—using the fundamental divisibility lemma— that $d = 1$, i.e., that r is an old-fashioned integer.

Corollary 1 *(***Theaetetus's Theorem***) The square root of any integer that is not a perfect square is irrational. E.g., $\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6} \ldots$ are irrational.*

For historical discussion about this see my article *How did Theaetetus prove his theorem?* on my web-page.

Proposition 2 *For any algebraic number α there is a positive integer $N \in \mathbf{Z}$ such that $N \cdot \alpha$ is an algebraic integer.*

I'll state a theorem that we will not prove right now but is our motivation for studying the rings of the two types:

$$\textbf{Type I}: \quad \mathbf{Z}[\sqrt{D}] := \{a + b\sqrt{D} \;\;|\;\; a, b \in \mathbf{Z}\} \subset \mathbf{Q}(\sqrt{D})$$
$$\text{for } D \text{ squarefree, not a perfect square, and not} \equiv 1 \bmod 4$$

$$\textbf{Type II}: \quad \mathbf{Z}[\delta] \quad = \quad \mathbf{Z}[\frac{1+\sqrt{D}}{2}] := \{a + b(\frac{1+\sqrt{D}}{2}) \;\;|\;\; a, b \in \mathbf{Z}\} \subset \mathbf{Q}(\sqrt{D})$$
$$\text{for } D \text{ squarefree, not a perfect square, and} \equiv 1 \bmod 4.$$

Theorem 2 *

- *If D is of "type I" as above the full ring of integers in $\mathbf{Q}(\sqrt{D})$ is $\mathbf{Z}[\sqrt{D}]$.*
- *If D is of "type II" the full ring of integers is $\mathbf{Z}[\delta] \quad = \quad \mathbf{Z}[\frac{1+\sqrt{D}}{2}]$.*

3 Recall tilings, and division with remainder

Consider the **tile**

$$\Omega := \{r + s \cdot \delta \mid -1/2 \leq r, s < 1/2\} \subset \mathbf{R}[\delta] \simeq \mathbf{R} \times \mathbf{R}.$$

We have the following tiling of the Euclidean plane:

$$\mathbf{R}[\delta] = \Omega + \mathbf{Z}[\delta] = \{\rho + \alpha \mid \rho \in \Omega; \;\alpha \in \mathbf{Z}[\delta]\}.$$

In other words, after adding an appropriate element of the lattice $\mathbf{Z}[\delta]$, we can "bring any element of $\mathbf{R}[\delta]$, and hence also of the field $\mathbf{Q}[\delta]$ into the *tile* Ω.

Problem 1: For which (square-free) values of D do we have that every element of the tile Ω (corresponding to D as above) have norm of absolute value strictly less than 1?

4 Euclidean Domains

Definition 2 *An integral domain A is called* **Euclidean** *if there is a function*

$$\lambda : A - \{0\} \to \mathbf{N}$$

with the following two properties:

1. *$\lambda(a) \le \lambda(ab)$ for all nonzero $a, b \in A$,*
2. *$a, b \in A$ with $b \neq 0$ we can find m and r in A such that*

$$a = mb + r$$

where $r = 0$ or $\lambda(r) < \lambda(b)$

Discuss *Norm-Euclidean* versus *Euclidean.*

Problem 2: When every element of the tile Ω (corresponding to D as above) has norm of absolute value strictly less than 1 show that $\mathbf{Z}[\sqrt{D}]$ (in case I) or $\mathbf{Z}[\delta]$ i(in case II) is a Euclidean domain.

If $a \in A$ I'll refer to $\lambda(a) \in \mathbf{N}$ as the "λ-value" of a.

Proposition 3

1. *Any two associate elements in $A - \{0\}$ have the same λ-value.*
2. *The group of units in A is the set of elements in $A - \{0\}$ of smallest λ-value.*
3. *Any nontrivial ideal I of A is generated by any element in I with the property that it has the smallest λ-value among all nontrivial elements of I.* **Note:** *Since any two generators of the same nontrivial ideal are associate elements and any two associate elements generate the same ideal, this means that there is a one:one correspondence*

   $\{$**Classes of (nonzero) associate elements of** $A\}$ $\leftrightarrow$ $\{$ **Nontrivial ideals of** $A\}$
4. *Every ideal of A is principal (i.e., is generated as ideal by a single element).*
5. *A Euclidean domain is a Principal Ideal Domain (meaning that it satisfies the property of the previous item).*
6. *The set of associativity classes of divisors of any nontrivial element is finite.*
7. *Any nontrivial, nonunit, element of A factors as a finite product of prime elements.*
8. *Any nontrivial element of A factors "uniquely" as a product of prime elements (or in parlance: A is a UFD).*

Discuss. Talk about PID's. GCD's as linear combos. Factorization in a PID. Discuss the group of units, and the equations:

$$X^2 + DY^2 = \pm 1.$$
$$X^2 + XY + CY^2 = \pm 1.$$

(where $C = \frac{1-D}{4}$)

Problem 3: Show that the group of units in the ring of integers of $\mathbf{Q}[\sqrt{2}]$ is infinite.

5 General comments on Quadratic Fields whose ring of integers are UFDs.

We have proved that:

Corollary 3 *The rings of integers in $\mathbf{Q}[\sqrt{D}]$ are Euclidean (and hence PID's and UFD's) when $D = -3, -2, -1, 2, 5$.*

But what is the real story?

Negative D: These are the *only* negative (square-free, non-square) D's such that the ring of integers in $\mathbf{Q}(\sqrt{D})$ is a PID (hence UFD)

$$-1, -2, -3, -7, -11, -19, -43, -67, -163.$$

Nine of them; talk about the history of the possible *tenth*.

Positive D: These are the first few positive (square-free, non-square) D's such that the ring of integers in $\mathbf{Q}(\sqrt{D})$ is a PID (hence UFD) :

$2, 3, 5, 6, 7, 11, 13, 14, 17, 19, 21, 22, 23, 29, 31, 33, 37, 38, 41, 43, 46, 47, 53, 57, 59, 61, 62, 67, 69, 71, 73, 77, 83, 86, 89, \ldots$

Infinitely many of them? This is an *Open Problem.* A conjecture (the Cohen-Lenstra heuristic) predicts that a bit over 3/4 of all positive D's (satisfying our conditions) have the property that the ring of integers in $\mathbf{Q}(\sqrt{D})$ is a PID (hence UFD), and computations seem to show this, but we can't even show that there are infinitely many D's with this property.