Algebraic Numbers, Algebraic Integers

October 7, 2012

1 Reading Assignment:

1. Read [**I-R**]Chapter 13, section 1.
2. Suggested reading: Davenport IV sections 1,2.

2 Homework set due October 11

1. Let p be a prime number. Show that the polynomial $f(X) = X^{p-1} + X^{p-2} + X^{p-3} + \ldots + 1$ is irreducible over $\mathbf{Q}$. Hint: Use *Eisenstein's Criterion* that you have proved in the Homework set due today; and find a change of variables, making just the right substitution for X to turn $f(X)$ into a polynomial for which you can apply Eisenstein' criterion.
2. Show that any unit not equal to ± 1 in the ring of integers of a real quadratic field is of infinite order in the group of units of that ring.
3. **[I-R]** Page 201, Exercises 4,5,7,10.
4. Solve Problems 1,2 in these notes.

3 Recall: Algebraic integers; rings of algebraic integers

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

Proposition 1 *Let $\theta \in \mathbf{C}$ be an algebraic integer. The minimal*[1] *monic polynomial $f(X) \in \mathbf{Q}[X]$ having θ as a root, has integral coefficients; that is, $f(X) \in \mathbf{Z}[X] \subset \mathbf{Q}[X]$.*

[1] i.e., minimal degree

Proof: This follows from the fact that a product of *primitive polynomials* is again primitive. Discuss. Define **content**.

Note that this means that there is no ambiguity in the meaning of, say, *quadratic algebraic integer*. It means, equivalently, a *quadratic number* that is an algebraic integer, or number that satisfies a quadratic monic polynomial relation with integral coefficients, or:

Corollary 1 *A quadratic number is a quadratic integer if and only if its trace and norm are integers.*

4 Rings of Quadratic Integers

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

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

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 $\mathbf{Z}[\delta] \quad = \quad \mathbf{Z}[\frac{1+\sqrt{D}}{2}]$.*

5 Recall: Gaussian Integers

We proved that the ring of Gaussian integers has the unique factorization property. Recall units, and the norm $N(a + ib) = a^2 + b^2$. Recall:

$$N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta).$$

Imagine, for some prime number p that you have a congruence:

$$A^2 + B^2 \equiv 0 \bmod \text{p},$$

with $A \not\equiv 0 \bmod \text{p}$

1. What do you know about such a prime p? (i.e., give a simple condition that p must satisfy.
2. Do all primes satisfying the above condition admit such a congruence?
3. Can you "use" such a congruence to get a pair of integers $0 < a \leq b$ such that

$$a^2 + b^2 = p?$$

4. Is this pair unique?

6 Recall tilings, and division with remainder

It is best, first, to suppose that we are in the case of complex quadratic numbers; i.e., $D < 0$. As we go through this, think of what you might have to do if you wanted an analogous theory for real quadratic numbers.

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?

Discuss the theory for real quadratic fields.

7 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. *$\lambda(a) \leq \lambda(ab)$ 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 2 *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*

   $$\{\textbf{Classes of (nonzero) associate elements of } A\} \quad \leftrightarrow \quad \{\ \textbf{Nontrivial ideals of } A\}$$

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

8 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.

9 How the Euclidean algorithm, Pell's Equation, Units in real quadratic fields, and continued fractions are all related