September 19:

Math 432 Class Lecture Notes

- Algebraic integers
- $\mathbf{Z}[i]$
- PID's and UFD's
- $\mathbf{Z}[i]$ again
- Pythagorean triples

0.1 Algebraic Integers

Now we use the theorem, from last time, that characterized algebraic integers, to prove that algebraic integers in a number field form a ring.

Theorem 1. If F is a number field and $\alpha, \beta \in \mathbf{Z}_F$ then $\alpha + \beta, \alpha\beta \in \mathbf{Z}_F$.

Proof. If

$$\mathbf{Z}[\alpha] = \mathrm{span}_{\mathbf{Z}}(1, \alpha, \alpha^2, \cdots, \alpha^{m-1}), \qquad \mathbf{Z}[\beta] = \mathrm{span}_{\mathbf{Z}}(1, \beta, \beta^2, \cdots, \beta^{n-1})$$

then $\mathbf{Z}[\alpha, \beta]$, which is defined to be the smallest subring of F containing α and β, is spanned by $\alpha^i\beta^j$ for $0 \leq i < m$, $0 \leq j < n$. By using the minimal polynomials for α and β one checks that $\alpha\mathbf{Z}[\alpha, \beta] \subset \mathbf{Z}[\alpha, \beta]$ and, similarly, that $\beta\mathbf{Z}[\alpha, \beta] \subset \mathbf{Z}[\alpha, \beta]$. It follows that $(\alpha + \beta)\mathbf{Z}[\alpha, \beta] \subset \mathbf{Z}[\alpha, \beta]$ and that $\alpha\beta\mathbf{Z}[\alpha, \beta] \subset \mathbf{Z}[\alpha, \beta]$ so that $\alpha + \beta$ and $\alpha\beta$ are algebraic integers as claimed. □

0.2 $\mathbf{Z}[i]$

Claim: $\mathbf{Z}[i] = \mathbf{Z}[\sqrt{-1}] = \mathbf{Z}_{\mathbf{Q}(i)}$ is a Euclidean domain with respect to the norm $N(a+bi) = a^2+b^2 = (a+bi)(a-bi)$.

This means that for all $x, y \in \mathbf{Z}[i]$ with $y \neq 0$, there exist $q, r \in \mathbf{Z}[i]$ such that $x = qy + r$ and $N(r) < N(y)$.

To prove this we find an algebraic integer that is "close" to the actual quotient. Let $x/y = A + Bi$ where $A, B \in \mathbf{Q}$. Let a be a nearest integer to A and b be a nearest integer to B. Then we see $q = a + bi$ and $r = x - qy$. Then

$$\begin{aligned} N(r) &= N(y(\frac{x}{y} - q)) = N(y)N((A-a)+(B-b)i) \\ &= N(y)[(A-a)^2 + (B-b)^2] \leq \frac{1}{2}N(y) < N(y). \end{aligned}$$

This finishes the proof that the "Gaussian integers" are a Euclidean domain.

By an argument that has become familiar (since we've seen it for the ring $\mathbf{Z}$ of integers and the ring $F[x]$ of polynomials over a field), we know that this implies that $\mathbf{Z}[i]$ is a principal ideal domain (PID).

In brief, if I is a nonzero ideal, choose $y \in I$ with the smallest positive norm. If $x \in I$ then $x = qy + r$ where $r \in I$. However $N(r) < N(y)$ so $r = 0$ and $x \in (y)$.

0.3 PID's and UFD's

By a standard result from elementary ring theory, any PID is a UFD. To understand what this means, we have to recall some definitions.

Two elements x, y are called associates in a ring R if $x = uy$ where $u \in R^*$ is a unit. An element $x \in R$ is called irreducible if $x = yz$ means y or z is an associate of x. An element x is prime if $x|ab$ means $x|a$ or $x|b$. If $x \neq 0$ then $x = u\prod p_i$ where $u \in R$ and all the p_i's are prime.

In a PID, one shows that any prime is an irreducible, any irreducible is prime, that every element can be factored as a product of primes, and that this factorization is unique in the sense that the primes in any two factorizations are essentially the same in that they differ only by replacing primes by associate primes.

Thus it is of some interest to describe the primes, and units, of a PID.

In the case of the integers **Z** the primes are the usual primes (or their negatives) and the units are $\{\pm 1\}$.

In the case of the ring of polynomials $F[x]$ over a field, the primes are the irreducible polynomials and the units are the nonzero scalars.

0.4 $\mathbf{Z}[i]$ again

In $\mathbf{Z}[i]$ we start by finding the units.

Lemma 2. $\mathbf{Z}[i]^* = \{\pm 1, \pm i\}$.

Proof. If $u \in \mathbf{Z}[i]^*$ then $\exists v \in \mathbf{Z}[i]^*$ such that $uv = 1$. This means $N(uv) = N(u)N(v) = 1$ or $N(u) = a^2 + b^2 = 1$. Thus we have either $a = 0, b = \pm 1$ or $b = 0, a = \pm 1$. □

Now we look at primes in $\mathbf{Z}[i]$. If $N(a+bi)$ is prime then $a+bi$ is a prime. Indeed, if

$$a + bi = uv$$

for algebraic integers u and v then by taking norms we see that

$$N(a + bi) = p = N(u)N(v)$$

which implies that $N(u) = 1$ or $N(v) = 1$ (since the norm of an algebraic integer is an integer), so that u or v is a unit.

Thus $2 + i$, which has norm 5, is a unit. In particular,

$$5 = (2 + i)(2 - i)$$

is not a prime. In fact, it $2 + i$ and $2 - i$ are not associates, so 5 factors as the product of two primes.

Similarly, $2 = (1 + i)(1 - i)$, and one checks that each of the factors are prime (since they have norm 2). However, $i(1 - i) = 1 + i$ so these factors are associates, and 2 is, roughly, the square of a prime.

On the other hand, one checks that if $p \equiv 3 \bmod 4$ is a prime then $N(a + bi) = p$ is impossible, since squares of integers are congruent to 0 or 1 mod 4, so that the sum of two squares is congruent to 0, 1, or 2 mod 4. Thus 3 and 7 are primes in $\mathbf{Z}[i]$.

Later we will show that any prime p that is 1 mod 4 can be written as the sum of two squares, $p = a^2 + b^2$.

If u is any prime element in $\mathbf{Z}[i]$, then $uu' = n$ is an integer and u is a divisor of a rational integer. Since all divisors of primes have been accounted for, this means that u is one of the prime discovered above.

We summarize these results (which have been completely proved, *except* for the factorization of primes congruent to 1 mod 4).

Theorem 3. The prime elements of $\mathbf{Z}[i]$ are associates of one of the following:

- $1 + i$
- p, where $p \equiv 3 \bmod 4$, p is a prime in $\mathbf{Z}$
- $a + bi$, where $a^2 + b^2$ is a prime congruent to 1 mod 4.

0.5 Pythagorean triples

As an amusing exercise, one can use the fact that $\mathbf{Z}[i]$ is a UFD to find all solutions to

$$x^2 + y^2 = z^2$$

in integers.

Suppose that x, y, z are nonzero integers that satisfy this equation. If any two have a common factor, then this factor divides the third. So after factoring out a common factor we can assume that any two are relatively prime. Then x and y are not both odd (since then z^2 would be 2 mod 4). So we can assume, without loss of generality that x is odd and y is even.

In $\mathbf{Z}[i]$ the equation becomes

$$(x + iy)(x - iy) = z^2.$$

Any divisor of $x+iy$ and $x-iy$ divides their sum $2x$ and their difference $2iy$. Since x and y are relatively prime (in $\mathbf{Z}$ or $\mathbf{Z}[i]$) it follows that any common factor divides 2. However, the fact that x is odd while y is even shows that $x + iy$ is not divisible by $1 + i$, the only nontrivial divisor of 2.

Thus $x + iy$ and $x - iy$ are relatively prime. The only way that relatively prime elements of a UFD can multiply to a square is if each is a square. The equation

$$x + iy = (a + bi)^2$$

implies that $x = a^2 - b^2$ and $y = 2ab$.

These observations can be summarized as follows.

Theorem 4. If x, y, z are integers such that $x^2 + y^2 = z^2$ then there are integers a, b, c such that a and b have opposite parity and either

$$x = (a^2 - b^2)c, \quad y = 2abc, \quad z = (a^2 + b^2)c$$

or the same equations hold, with x and y reversed.