Math 431 homework Discussion Due Friday, October 26, 2001

1. Let $I = (2, 1 + \sqrt{-3}) \subset \mathbf{Z}[\sqrt{-3}]$. Show that $I^2 = 2I$. Why does this not contradict unique factorization of ideals in a Dedekind domain?

Discussion. The product of two ideals is generated by all possible products of pairs of generators. So

$$I^2 = (4, 2(1 + \sqrt{-3}), -2 + 2\sqrt{-3}) = (4, 2 + 2\sqrt{-3}) = 2I.$$

This does not contract unique factorization in a Dedekind ring because $\mathbf{Z}[\sqrt{-3}]$ isn't a Dedekind domain.

2. Let $F = \mathbf{Q}(\alpha)$, where $\alpha^3 - \alpha^2 - 2\alpha - 8 = 0$. Show that $\mathbf{Z}_F = \mathrm{span}_{\mathbf{Z}}(1, \alpha, (\alpha^2 + \alpha)/2)$. Find three nontrivial ring homomorphisms from $\mathbf{Z}_F$ to $\mathbf{Q}_2$.

Discussion. The fab $L := \mathrm{span}_{\mathbf{Z}}(1, \alpha, (\alpha^2 + \alpha)/2)$ satisfies

$$\mathbf{Z}[\alpha] \subset_{\neq} L \subset \mathbf{Z}_F.$$

From the formula

$$\mathrm{disc}(1, \alpha, \alpha^2) = [\mathbf{Z}_F : \mathbf{Z}[\alpha]] \, \mathrm{disc}(\mathbf{Z}_F)$$

and a calculation that the discriminant of the minimal polynomial for α is $-2^2 \cdot 503$ (note: the formula for the discriminant of a general monic cubic is in the class notes on resultants and discriminants), we see that the index of $\mathbf{Z}[\alpha]$ in $\mathbf{Z}_F$ must be 2, and that $L = \mathbf{Z}_F$.

If we let $\beta = (\alpha^2 + \alpha)/2$, then $\mathbf{Z}_F = \mathrm{span}_{\mathbf{Z}}(1, \alpha, \beta)$. As can be checked by computing $\alpha\beta$ and β^2, the ring structure is given by the rules

$$\alpha^2 = -\alpha + 2\beta, \quad \alpha\beta = 2\beta + 4, \quad \beta^2 = 2\alpha + 3\beta + 6.$$

In order to define a homomorphism from $\mathbf{Z}_F$ to $\mathbf{Q}_2 = \{0, 1\}$ we have to map rational integers to their residues mod 2, and map map each of α and β to 0 or 1. So there are nominally four possibilities. A quick glance at the multiplication rules shows that mapping α and β both to 1 would contradiction the multiplication rule for $\alpha\beta$, but that every other possibility gives a homomorphism. Thus there are three homomorphisms all together. Note that the kernel of each of this is a prime ideal of index (norm) equal to 2.

Digression: This explains why the field $\mathbf{Q}(\alpha)$ has no power basis. The prime 2 splits into three prime ideals of degree 1. *If* there was a power basis, then the minimal polynomial of the generator would have to factor into the product of three irreducible polynomials of degree 1 modulo 2. Unfortunately, there are only two such irreducible polynomials, x and $x + 1$.

3. Show that any Dedekind domain with finitely many prime ideals is a PID. (Hint: Use the CRT to find a generator of an ideal.)

Discussion. One way to do this is to show that each prime ideal P is principal. Choose an element β in P but not in P^2. (This is possible since factorization into primes is unique, so P and P^2 are distinct ideals.) Now use the Chinese Remainder Theorem to chose an element α that is congruent to β modulo P^2

and congruent to 1 modulo all of the (finitely many) other prime ideals. By construction the principal ideal (α) is equal to P, and P is principal, as desired.

4. Show that if I is any ideal in a number ring $\mathbf{Z}_F$ then $\mathbf{Z}_F/I$ is a PID.

Discussion. There is a one-to-one correspondence between ideals $\overline{J}$ in the quotient ring and ideals J in $\mathbf{Z}_F$ that contain I. Given such an ideal $\overline{J}$, and a corresponding ideal J, chose a nonzero element of I, and then apply our "two-generator" theorem from class to find a β such that $J = (\alpha, \beta)$. Since α is in I, we see that in the quotient α vanishes, and $\overline{J} = (\overline{\beta})$ so that $\overline{J}$ is principal as desired.

The ring $\mathbf{Z}_F/I$ need *not* be a Dedekind domain, since, for instance, it might not even be an integral domain.

5. Let $F = \mathbf{Q}(\alpha)$ where $\alpha^3 + \alpha + 1 = 0$. Show that in the ring $\mathbf{Z}_F$

$$(3) = PQ, \text{ where } P = (3, \alpha + 2), Q = (3, \alpha^2 + \alpha + 2)$$

$$(31) = P^2Q, \text{ where } P = (31, \alpha - 14), Q = (31, \alpha - 3).$$

For the primes over 3 we have

$$PQ = (9, 3\alpha + 6, 3\alpha^2 + 3\alpha + 6, 3\alpha^2 + 3\alpha + 3).$$

The difference of the last two generators is 3, and since every other generator is a multiple of 3 we have $PQ = (3)$.

For the primes over $p = 31$ we have $P^2 = (p^2, p(\alpha - 14), \alpha^2 - 28\alpha + 196)$ and

$$\begin{aligned} P^2Q &= (p^3, p^2(\alpha - 14), p(\alpha^2 - 28\alpha + 196), p^2(\alpha - 3), && (1) \\ &\quad p(\alpha^2 - 17\alpha + 42), p(-\alpha^2 + 9\alpha + 19)). && (2) \end{aligned}$$

There are three generators that are nominally divisible by p. We eliminate the α^2 terms by subtracting the first two of these to give $u = p(-11\alpha + 154)$. Adding the last two of these gives $v = p(-8\alpha + 23)$. To eliminate the α term we calculate $8u - 11v = -979p$. Since 979 is not divisible by p, the gcd of $979p$ and p^3 is p, so a suitable linear combination of those elements is equal to p. And since every element is divisible by p, we conclude that $(p) = P^2Q$.