Math 431 Quiz October quiz Discussion

1. Let α be a root of $f(x) = x^3 - 4x - 1$ and let $F = \mathbf{Q}(\alpha)$. Prove that $\mathbf{Z}_F = \mathbf{Z}[\alpha]$. Find a unit in $\mathbf{Z}_F$. Show that $2\mathbf{Z}_F$ is not a prime ideal (hint: to find two algebraic integers whose product is in the ideal, you could choose one of them to be $\alpha + 1$.) Find $\mathrm{Tr}_{F/\mathbf{Q}}(\alpha^k)$ for $k = 0, 1, 2, 3$.

Discussion. From our formula for the discriminant of a cubic polynomial,

$$\mathrm{disc}(x^3 - 4x - 1) = -4(-4)^3 - 27(-1)^2 = 229.$$

By formulas in class this is equal to

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

Since 229 is *squarefree* (in fact, a prime) the index on the *RHS* must be equal to 1, and we conclude that $\mathbf{Z}_F = \mathbf{Z}[\alpha]$ and $\mathrm{disc}(\mathbf{Z}_F) = 229$.

The element α is itself a unit, as can be seen directly either from

$$\alpha(\alpha^2 - 4) = 1$$

or the form equation

$$N_{F/\mathbf{Q}}(\alpha - m) = -\prod_{i=1}^{3}(m - \alpha^{(i)}) = -f(m)$$

so that $N(\alpha) = -f(0) = 1$. Since $f(2) = -1$ we also see that $\alpha - 2$ is a norm.

To show that $2\mathbf{Z}_F = (2)$ is not a prime ideal we have to find two elements of the ring that are not in the ideal but whose product is in the ideal. Many things work, e.g., using the equation satisfied by α we find that

$$4\alpha = \alpha^3 - 1 = (\alpha - 1)(\alpha^2 + \alpha + 1)$$

and the two factors on the *RHS* are certainly not in $2\mathbf{Z}[\alpha]$.

The trace of α^k is the sum of the k-th powers of the conjugates of α, i.e, it is the power sum p_k if the "x_i" are the conjugates of α. The elementary symmetric functions are the coefficients of the minimal polynomial satisfied by α, and we find that $e_1 = 0$, $e_2 = -4$, $e_3 = 1$. From the equations discussed earlier

$$p_1 - e_1 = 0, \quad p_2 - e_1 p_1 + 2e_2 = 0, \quad p_3 - e_1 p_2 + e_2 p_1 - 3e_3 = 0$$

we discover that $p_1 = 0$, $p_2 = 8$, $p_3 = 3$. The later trace could also be calculated by using the additivity of the trace: since $\alpha^3 = 4\alpha + 1$ we have

$$\mathrm{Tr}(\alpha^3) = \mathrm{Tr}(4\alpha + 1) = 4\mathrm{Tr}(\alpha) + \mathrm{Tr}(1) = 3.$$

If needed, traces of higher powers can be computed using the recursion

$$p_{n+3} - e_1 p_{n+2} + e_2 p_{n+1} - e_3 p_n = 0.$$

2. Let $u_0, u_1, \cdots$ be a sequence of integers (i.e., elements of $\mathbf{Z}$) such that

$$u_{n+3} - 4u_{n+1} - u_n = 0$$

for all $n \geq 0$. Prove that there are numbers a_i so that

$$u_n = \sum_{i=1}^{3} a_i \left(\alpha^{(i)}\right)^n$$

where α is as given in the previous problem. (Hint: consider the first 3 terms and the *** matrix.) What can you say about

$$\lim_{n\to\infty} |u_n|^{1/n} \quad ?$$

Discussion. Constant coefficient linear recursions are often treated in linear algebra. One finds that if the recurrence "has distinct eigenvalues" then the n-th term is a linear combination of the n-powers of the roots of the characteristic polynomial. This can be verified directly. The linear equations for three variables a_i

$$\begin{bmatrix} u_0 \\ u_1 \\ u_2 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ \alpha^{(1)} & \alpha^{(2)} & \alpha^{(3)} \\ \left(\alpha^{(1)}\right)^2 & \left(\alpha^{(2)}\right)^2 & \left(\alpha^{(3)}\right)^2 \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

can obviously be solved (the coefficient matrix is a Vandermonde, and the fact that the conjugates of α are distinct implies that the matrix is nonsingular). Thus the equation

$$u_n = a_1 \left(\alpha^{(1)}\right)^n + a_2 \left(\alpha^{(2)}\right)^n + a_3 \left(\alpha^{(3)}\right)^n$$

is true for $n = 0, 1, 2$. Since the sequences u_n and α^n satisfy the same recursion it follows that the formula is true for all n.

The asymptotic behavior of the sequence is determined by the relative relationship of the roots $\alpha^{(i)}$. A quick glance at the polynomial shows that there is a real root between 2 and 3 (actually, much closer to 2 since $f(2) = -1$ and $f(3) = 14$; the root can be isolated quite accurately by Newton's method, and one finds XXX). Since the product of the roots is equal to 1, the other two complex conjugate roots have absolute value in the vicinity of 2/3. We find that

$$|u_n|^{1/n} = |a_1|^{1/n}\alpha^{(1)}|1 + (a_2/a_1)(\alpha^{(2)}/\alpha^{(1)})^n + (a_3/a_1)(\alpha^{(3)}/\alpha^{(1)})^n|^{1/n}$$

where the numbering is chosen so that $\alpha^{(1)}$ is the real root. This assumes that the u_i are not identically 0; using this, and also the fact that a_1 isn't 0 (which can be verified in several ways), the limit is immediately seen to be $\alpha^{(1)}$.

3. Describe all solutions to the diophantine equation

$$x^2 + xy - 8y^2 = 1.$$

Discussion. Since the discriminant of the quadratic form on the left is 33, we expect that $\mathbf{Q}(\sqrt{33})$ should have something to do with this. If $\delta = (1 + \sqrt{33})/2$

then $\delta + \delta' = 1$, $\delta\delta' = -8$, and δ satisfies the equation $\delta^2 - \delta - 8 = 0$. Moreover, the quadratic form in the problem turns out to conveniently be the norm form:

$$N(x + y\delta) = (x + y\delta)(x + y\delta') = x^2 + xy - 8y^2.$$

Thus we are being asked to find units of norm 1 in the real quadratic field $\mathbf{Q}(\sqrt{33})$.

Inspecting the equation $g(x, y) = x^2 + xy - 8y^2 = 1$ we see that x must be odd and y even. Since $g(x, -y) = g(x - 1, y)$ it suffices to consider positive y. Moreover, writing the equation in the form $(2x + y)^2 - 33y^2 = 4$ one easily checks that $y \equiv \pm 1 \bmod 5$ won't work, since then $y^2 \equiv 1 \bmod 5$ and we would have a square being congruent to 2 modulo 5, which is impossible. Thus the first two possible values of y to try are $y = 2$ and $y = 8$. Fortunately, the second of these works, and we find that $x = 19$, $y = 8$ is a solution.

Is the unit $19 + 8\delta$ fundamental? In fact, since 8 is the smallest value of y that works, it isn't too hard to show that the unit is fundamental (this is a general fact in quadratic fields: the first y value that works is fundamental). However, later we will need to be able to verify that units that we find by other means are fundamental, so we will work through the procedure discussed in class. Namely, any fundamental unit is larger than $\sqrt{D - 3} = \sqrt{30}$. The cube root of $u = 19 + 8\delta$ is smaller than $\sqrt{30}$, so either u is fundamental or else it is the square of a fundamental unit. The equation

$$(a + b\delta)^2 = 19 + 8\delta$$

leads to $a^2 + 8b^2 = 19$ which is impossible to solve in integers, so u is fundamental.

Thus all units are of the form $\pm u^k$, for $k \in \mathbf{Z}$. Another way to describe them is by saying that a string of solutions are defined recursively by the equations $x_1 = 19$, $y_1 = 8$ and

$$x_{n+1} = 19x_n + 64y_n, \qquad y_{n+1} = 8x_n + 27y_n$$

(multiplying $u^n = x_n + y_n\delta$ by $19 + 8\delta$ and using $\delta^2 = \delta + 8$ given above). And that all other solutions are of the form $(-x_n, -y_n)$, by taking the negatives, or $(x_n + y_n, -y_n)$, by taking conjugates.

4. Show that if a polynomial with rational coefficients has r_1 real roots and r_2 pairs of complex conjugate roots, then the sign of its discriminant is $(-1)^{r_2}$. (Hint: One easy way to do this is to factor the polynomial over $\mathbf{R}$, and then use formulae.) Show that if F is a number field with r_1 real embeddings and r_2 pairs of complex conjugate embeddings then the sign of its discriminant is $(-1)^{r_2}$.

Discussion. The formula $\mathrm{disc}(fg) = \mathrm{disc}(f)\mathrm{disc}(g)Res(f, g)^2$ implies that the sign of the discriminant of polynomials is equal to the product of signs of the discriminants of the polynomials. Over the real numbers, a polynomial with rational (or real) coefficients factors into linear factors $x - a$ and quadratic factors

x^2+ax+b that have complex conjugate roots (i.e., satisfying $a^2-rb<0$). The discriminant of a linear polynomial $x-a$ is equal to 1. The discriminant of a quadratic with complex conjugate roots is negative. Putting this all together, we see that the discriminant of a polynomial as described is positive if and only if the number r_2 of pairs of complex conjugate roots (i.e., the number of quadratic factors over $\mathbf{R}$) is even.

If $F = \mathbf{Q}(\alpha)$ (which is is always the case, for some α, by the Primitive Element Theorem) and we assume that α is an algebraic integer, then we know that

$$\operatorname{disc}(F) = \operatorname{disc}(\mathbf{Z}_F) = \operatorname{disc}(\mathbf{Z}[\alpha])/[\mathbf{Z}_F : \mathbf{Z}[\alpha]]^2$$

and that the discriminant of $\mathbf{Z}[\alpha]$ is the discriminant of its minimal polynomial. Thus the sign of disc(F) is equal to the sign of the discriminant of a generator¿α and is equal to $(-1)^{r_2}$.

5. Show that if I is a nonzero ideal in the ring of integers $\mathbf{Z}_F$ of a number field then $I \cap \mathbf{Z}$ is a nonzero ideal in $\mathbf{Z}$.

Discussion. The intersection of I and $\mathbf{Z}$ satisfies the conditions for being an ideal, so it suffices to show that there is a nonzero element in the intersection. One way to see this is to observe that the norm of α is in the intersection, and another (equivalent) way is to observe that if the minimal polynomial of α has the shape

$$x^n + a_1 x^{n-1} + \cdots + a_0 = 0$$

then a_0 is in the ideal generated by α, and a_0 is nonzero.

6. For each prime ideal P in $\mathbf{Z}[i]$ (see the class notes for 9/21 for an explicit list) find, with explanation, the index $[\mathbf{Z}[i] : P]$ of P in $\mathbf{Z}[i]$.

Discussion. One can find explicit coset representatives without too much difficulty, but it is easy just to use the result from class saying that the index of a sub-fab is the absolute value of the determinant of the change of basis matrix. The ideals of the form $P = (a+bi)$ where $a^2+b^2 = p$ is a prime (which includes the ideal $(1+i)$ which contains 2) clearly have basis $a+bi$, and $i(a+bi) = -a+bi$. The determinant of the changes of basis matrix is $a^2+b^2 = p$.

Ideals of the form (p) where p is a rational prime have basis p, pi and the determinant of the change of basis matrix is p^2.

In all cases, we have $[\mathbf{Z}[i] : I] = N(x)$ if I is a prime ideal generated by x.

7. Let α and β be algebraic integers of degree n that satisfy

$$\operatorname{Tr}_{\mathbf{Q}(\alpha)/\mathbf{Q}}(\alpha^k) = \operatorname{Tr}_{\mathbf{Q}(\beta)/\mathbf{Q}}(\beta^k)$$

for $0 \le k \le n$. Prove that $\alpha = \beta$.

Discussion. The traces are power sums of α or β and their conjugates. Elementary symmetric functions can be determined recursively from the power sums, using Newton's identities. Thus the elementary symmetric functions of α and β are the same, and $alpha$ and β are roots of the same polynomial, and are conjugate, as desired.