Math 431 October 5 homework discussion

1. Find odd square-free integers a and b such that $(\sqrt{a}+\sqrt{b})/2$ is an algebraic integer.

Discussion. The minimal polynomial for $\sqrt{a}+\sqrt{b}$ is

$$x^4 - 2(a+b)x^2 + (a-b)^2.$$

So $(\sqrt{a}+\sqrt{b})/2$ is an algebraic integer if and only if $a+b$ is even and $a-b$ is divisible by 16. If a and b are both odd the first condition is automatic, and the second done is true if and only if a and b are congruent modulo 4. Of course, trivial examples exist, e.g., $a=b$. And this analysis shows that a random guess has a 50/50 chance of being right.

2. Prove that $D(fg) = D(f)D(g)\mathrm{Res}(f,g)^2$ where $D(f)$ denotes the discriminant of a polynomial f.

Discussion. It is fairly routine to express all quantities in terms of the roots of the polynomial. Here is an argument (not particularly shorter) that only uses properties of the resultant.

$$\begin{aligned} D(fg) &= \pm f_m^{-1} g_n^{-1} R(fg, fg' + f'g) \\ &= \pm f_m^{-1} g_n^{-1} R(f, fg' + f'g) R(g, fg' + f'g) \\ &= \pm f_m^{-1} g_n^{-1} R(f, f'g) R(g, fg') \\ &= \pm f_m^{-1} g_n^{-1} R(f, f') R(f, g) R(g, f) R(g, g') \\ &= \pm D(f) D(g) R(f, g)^2. \end{aligned}$$

Here the definition $D(f) = (-1)^{m(m-1)/2} f_m^{-1} R(f, f')$ has been used several times, the "quotient/remainder" property has been used, and multiplicativity has been used. The $\pm$ sign can be specified precisely and one finds that the final sign is

$$(-1)^{mn+m(m-1)/2+n(n-1)/2+(m+n)(m+n-1)/2} = 1.$$

3. Prove or disprove: If E and F are distinct cubic extensions of $\mathbf{Q}$, and K is a number field that contains both, then the degree of K over $\mathbf{Q}$ is divisible by 9.

Discussion. The conjugate fields $\mathbf{Q}(\sqrt[3]{2})$ and $\mathbf{Q}(e^{2\pi i/3}\sqrt[3]{2})$ both have degree 3 over $\mathbf{Q}$, but, as discussed in class, the splitting field $\mathbf{Q}(\sqrt[3]{2}, e^{2\pi i/3})$ contains both of them and has degree 6 over $\mathbf{Q}$. (In fact, if E and F are "unrelated" any field K will have degree divisible by 9.)

4. Prove that the discriminant of the polynomial $f(x) = x^n + ax + b$ is

$$D(f) = (-1)^{n(n-1)/2} n^n b^(n-1) + (-1)^{(n+2)(n+3)/2} (n-1)^{n-1} a^n.$$

Discussion. Properties of the resultant come to the rescue.

$$\begin{aligned}
D(x^n + ax + b) &= (-1)^{n(n-1)/2} R(x^n + ax + b, nx^{n-1} + a) \\
&= (-1)^{n(n-1)/2} R(nx^{n-1} + a, x^n + ax + b) \\
&= (-1)^{n(n-1)/2} n^n R(x^{n-1} + \frac{a}{n}, x(x^{n-1} + \frac{a}{n}) + \frac{(n-1)a}{n} + b) \\
&= (-1)^{n(n-1)/2} n^n R(x^{n-1} + \frac{a}{n}, \frac{(n-1)a}{n} + b) \\
&= (-1)^{n(n-1)/2} (-1)^n n^n R(\frac{(n-1)a}{n} + b, x^{n-1} + \frac{a}{n}) \\
&= (-1)^{n(n-1)/2} (-1)^n n^n \left((-b)^{n-1} + \frac{a}{n} \left(\frac{(n-1)a}{n} \right)^{n-1} \right) \\
&= (-1)^{n(n-1)/2} \left(n^n b^{n-1} + (-1)^{n-1} (n-1)^{n-1} a^n \right) \\
&= (-1)^{n(n-1)/2} n^n b^{n-1} + (-1)^{(n+2)(n+3)/2} (n-1)^{n-1} a^n
\end{aligned}$$

5. Show that $(1 - \zeta_8)^4$ is an associate of 2 in $\mathbf{Z}[\zeta_8]$ where $\zeta_8 = e^{2\pi i/8}$ is a primitive eighth root of unity.

Discussion. The minimal polynomial of ζ_8 is $f(x) = x^4 + 1$. The norm of $x - \zeta_8$ is $f(x)$ (see a later problem), so $N(1 - \zeta_8) = 2$. It is easy to verify the equation

$$(1 - \zeta_8)^4 = -4\zeta_8 + 6\zeta_8^2 - 4\zeta_8^3 = 2u$$

where $u = -2\zeta_8 + 3\zeta_8^2 - 2\zeta_8^3$; taking the norm of both sides shows that $N(u) = 1$. Thus u is a unit and 2 and $(1 - \zeta_8)^4$ are indeed associates.

6. Show that if $\mathrm{m}_\alpha(x) = x^3 - x - 2x^2 - 8$ and $F = \mathbf{Q}(\alpha)$ then

$$(\alpha^2 + \alpha)/2 \in \mathbf{Z}_F \backslash \mathbf{Z}[\alpha].$$

Discussion. There are several ways to find the equation of $\beta = \alpha^2 + \alpha$. One is to find β^2 and β^3 explicitly and find a linear dependence on $1, \beta, \beta^2, \beta^3$. Another is to find the matrix of multiplication by β (by multiplying β by

each of $1, \alpha, \alpha^2$ and expressing the results in terms of the same basis) and taking the characteristic polynomial of the matrix. Still another is to do the symmetric function exercise implicit in finding the coefficients of

$$f(x) = \prod_{i=1}^{3}(x - \alpha_i^2 - \alpha_i)$$

(where the α_i are the conjugates of α). Finally, one can compute the resultant

$$\mathrm{Res}_x(y - x^2 - x, x^3 - x^2 - 2x - 8)$$

to get a cubic in y. (The intuitive explanation is that in eliminating x between those two expressions we find an equation satisfied by y; the more precise explanation is that in taking the product of the expression $y - x^2 - x$ as x takes on the three different roots of m_α we are exactly computing $f(x)$ above.) We find (keeping in mind that signs are irrelevant)

$$\mathrm{Res}(x^2+x-y, x^3-x^2-2x-8) = \mathrm{Res}(x^2+x-y, (x-2)(x^2+x-y)+yx-2y-8)$$

$$= (2y+8)^2 + y(2y-8) - y \cdot y^2 = -(y^3 - 6y^2 + 40y - 64)$$

from which it follows that $\beta/2$ is an algebraic integer. Since $1, \alpha, \alpha^2$ is a basis of $\mathbf{Z}[\alpha]$ it is obvious that β is not in $\mathbf{Z}[\alpha]$.

7. Let p be an odd prime, $\zeta = e^{2\pi i/p}$, and $F = \mathbf{Q}(\zeta)$. Find $N_{F/\mathbf{Q}}(\zeta)$. Find $N_{F/\mathbf{Q}}(\zeta - 1)$.

Discussion. If $f(x) = \mathrm{m}_\alpha(x)$ for any algebraic α and r is any integer then

$$N_{\mathbf{Q}(\alpha)/\mathbf{Q}}(\alpha - r) = \prod_{i=1}^{n}(\alpha_i - r) = (-1)^n \prod_{i=1}^{n}(r - \alpha_i) = (-1)^n f(r).$$

The minimal polynomial of ζ is $1 + x + x^2 + \cdots + x^{p-1}$ and so we find that $N(\zeta) = 1$ and $N(\zeta - 1) = p$.

8. Let I be a nontrivial ideal in the ring of integers $\mathbf{Z}_F$ of a number field F. Prove that there is a nonzero element in $I \cap \mathbf{Z}$.

Discussion. If α is a nonzero element of I then $N(\alpha)$ is nonzero, and $N(\alpha) = \alpha\beta = m \in \mathbf{Z}$, where β is the product of the other conjugates of α. Since the other conjugates are algebraic integers, β is an algebraic integer, and the equation $\alpha\beta = m$ shows that β is in F. Thus $\beta \in \mathbf{Z}_F$ and $m \in I$.

Alternatively, the constant term of the minimal polynomial of α is easily seen to be in $I \cap \mathbf{Z}$. (This is no surprise: the constant term is equal to the norm, up to sign.)

9. Find an example of nonunique factorization in $\mathbf{Q}(\sqrt{-15})$. I.e., find an element that factors into irreducibles in two genuinely different ways.

Discussion. The ring of integers is $\mathbf{Z}[\delta]$, where $\delta = (1+\sqrt{-15})/2$; the norm form is $N(a+b\delta) = a^2+ab+4b^2$. Almost anything works as a counterexample; for instance

$$3 \cdot 5 = \sqrt{-15} \cdot \sqrt{15}.$$

To show that each element on both sides is irreducible, it suffices to show that no element has norm 3 or 5 (e.g., if 3 factors as $e = uv$, where u and v aren't units, then $9 = N(3) = N(u)N(v)$, so that u has norm 3), and this is easy from the norm form. Almost any