MATH 129, HW 3

Bryden Cais

February 26, 2002

1 Discriminant

1. We have

$$\begin{aligned} D(X^2+bX+c) &= \operatorname{Res}(2X+b, X^2+bX+c) = \begin{vmatrix} b & 0 & c \\ 2 & b & b \\ 0 & 2 & 1 \end{vmatrix} \\ &= -b^2+4c. \end{aligned}$$

2. (a) One direction is obvious: namely, if ψ is a bijection then since $1 \in K_{p+q-1}[X]$, there exist $A \in K_{q-1}[X]$ and $b \in K_{p-1}[X]$ such that $\psi(A, B) = 1$, that is $AP + BQ = 1$. This shows that $\gcd(P, Q) = 1$. Now conversely, suppose that $\gcd(P, Q) = 1$. If ψ is not injective, then there exist distinct $A_1,\ A_2 \in K_{q-1}[X]$ and $B_1,\ B_2 \in K_{p-1}[X]$ such that $A_1P + B_1Q = A_2P + B_2Q$, that is, $(A_1 - A_2)P = (B_2 - B_1)Q$. Clearly, $Q|(A_1 - A_2)P$. Since $\gcd(P, Q) = 1$ and $K[X]$ is Euclidean, we have $Q|(A_1 - A_2)$, which is impossible since $\deg(A_1 - A_2) \leq q - 1 < \deg(Q)$. Thus we see that ψ must be injective. Now since the map ψ is a K-vector space homomorphism and since $\dim_K(K_{q-1}[X] \times K_{p-1}[X]) = \dim_K(K_{p+q-1}[X])$, we see that ψ is also surjective, and hence bijective.

   (b) By the above, we know that $\gcd(P, Q) = 1$ iff ψ is a bijection. Since ψ is a K-linear map, ψ is a bijection iff the determinant of its matrix is not 0. Let $A = c_0 + c_1X + \cdots + c_{q-1}X^{q-1}$, $B = d_0 + d_1X + \cdots + d_{p-1}X^{p-1}$. Let $v \in K_{q-1}[X] \times K_{p-1}[X]$ be the column vector given by $c_0, \ldots, c_{q-1}, d_0, \ldots, d_{p-1}$. Then it follows from straightforward matrix multiplication that the $p+q-1$ column vector given by the coefficiens of $AP + BQ$ is equal to

$$\begin{pmatrix} a_0 & & & b_0 & & \\ a_1 & \ddots & & \vdots & \ddots & \\ \vdots & \ddots & a_0 & b_{q-1} & \ddots & b_0 \\ a_p & \ddots & a_1 & b_q & \ddots & \vdots \\ & \ddots & \vdots & & \ddots & b_{q-1} \\ & & a_p & & & b_q \end{pmatrix} v.$$

Thus, we see that the determinant of ψ is just the resultant $\mathrm{Res}(P, Q)$, and hence that ψ is a bijection iff $\mathrm{Res}(P, Q) \neq 0$.

(c) Let $P = a_p(X - \alpha_1) \cdots (X - \alpha_p)$, $Q = b_q(X - \beta_1) \cdots (X - \beta_q)$. Let $V(X_1, X_2, \ldots, X_n)$ denote the matrix

$$\begin{pmatrix} 1 & X_1 & \cdots & X_1^n \\ 1 & X_2 & \cdots & X_2^n \\ \vdots & \vdots & \cdots & \vdots \\ 1 & X_n & \cdots & X_n^n \end{pmatrix},$$

set $M = V(\beta_q, \cdots, \beta_1, \alpha_p, \cdots, \alpha_1)$ and

$$R = \begin{pmatrix} a_0 & & & b_0 & & \\ a_1 & \ddots & & \vdots & \ddots & \\ \vdots & \ddots & a_0 & b_{q-1} & \ddots & b_0 \\ a_p & \ddots & a_1 & b_q & \ddots & \vdots \\ & \ddots & \vdots & & \ddots & b_{q-1} \\ & & a_p & & & b_q \end{pmatrix}.$$

We first show that $\det(V(X_1, \ldots, X_n)) = \prod_{1 \leq i < j \leq n}(X_i - X_j)$. To see this, for $1 \leq j \leq n - 1$, subtract X_1 times the j th column from the $j + 1$ st column of the matrix $V(X_1, \ldots, X_n)$. These operations do not alter the determinant, and we find that

$$\det(V(X_1, \ldots, X_n)) = \prod_{2 \leq i \leq n} (X_i - X_1) \det(V(X_2, \ldots, X_n)).$$

Induction then gives the proposed formula. We now compute the determinant of MR in two different ways. It is not difficult to see that

$$\begin{pmatrix} 1 & \beta_q & \cdots & \beta_q^{p+q-1} \\ \vdots & \vdots & \cdots & \vdots \\ 1 & \beta_1 & \cdots & \beta_1^{p+q-1} \\ 1 & \alpha_p & \cdots & \alpha_p^{p+q-1} \\ \vdots & \vdots & \cdots & \vdots \\ 1 & \alpha_1 & \cdots & \alpha_1^{p+q-1} \end{pmatrix} \begin{pmatrix} a_0 & & & b_0 & & \\ a_1 & \ddots & & \vdots & \ddots & \\ \vdots & \ddots & a_0 & b_{q-1} & \ddots & b_0 \\ a_p & \ddots & a_1 & b_q & \ddots & \vdots \\ & \ddots & \vdots & & \ddots & b_{q-1} \\ & & a_p & & & b_q \end{pmatrix}$$

$$= \begin{pmatrix} P(\beta_q) & \cdots & P(\beta_q)\beta_q^{q-1} & & & \\ \vdots & \cdots & \vdots & & & \\ P(\beta_1) & \cdots & P(\beta_1)\beta_1^{q-1} & & & \\ & & & Q(\alpha_p) & \cdots & Q(\alpha_p)\alpha_p^{p-1} \\ & & & \vdots & \cdots & \vdots \\ & & & Q(\alpha_1) & \cdots & Q(\alpha_1)\alpha_1^{p-1} \end{pmatrix},$$

and hence that

$$\det(MR) = \det(V(\beta_q,\ldots,\beta_1)V(\alpha_p,\ldots,\alpha_1)) \prod_{1\le j\le q} P(\beta_j) \prod_{1\le i\le p} Q(\alpha_i).$$

On the other hand,

$$\begin{aligned} \det(MR) &= \det(M)\det(R) \\ &= \det(V(\beta_q,\ldots,\beta_1,\alpha_p,\ldots,\alpha_1))\mathrm{Res}(P,Q). \end{aligned}$$

Now, using our formula for the determinant of $V(X_1,\ldots,X_n)$, we see that

$$\begin{aligned} &\det(V(\beta_q,\ldots,\beta_1,\alpha_p,\ldots,\alpha_1)) \\ &= \det(V(\beta_q,\ldots,\beta_1))\det(V(\alpha_p,\ldots,\alpha_1)) \prod_{1\le i\le p}\prod_{1\le j\le q}(\alpha_i-\beta_j) \\ &= \det(V(\beta_q,\ldots,\beta_1))\det(V(\alpha_p,\ldots,\alpha_1)) \frac{1}{b_q^p} \prod_{1\le i\le p} Q(\alpha_i). \end{aligned}$$

It thus follows that

$$\mathrm{Res}(P,Q) = b_q^p\, P(\beta_1)\cdots P(\beta_q).$$

Notice that $\mathrm{Res}(P,Q) = (-1)^{pq}\mathrm{Res}(Q,P)$ since to swap the roles of the a_i's and the b_j's in the defining determinant of the resultant requires a bubble sort involving pq flips of columns.

3. Let $P \in K[X]$ with $\deg(P) > 0$. Clearly, P has only simple roots in $\bar{K}$ iff P, P' have no common roots. By part c above, this is the case iff $R(P', P) = D(P)$ is not zero. Thus a and c are equivalent. By part b above, $\gcd(P,\ P') = 1$ iff $D(P) \neq 0$, so that b and c are equivalent. Furthermore, if P has some root of multiplicity greater than 1 then we can write $P = Q^k R$ for $Q,\ R \in K[X]$ with $P \not| Q$, $\deg(Q) \geq 1$, and $k \geq 2$. Thus $QR \in K[X]/P$ is not zero and is nilpotent since $P|(QR)^k$. Thus, $K[X]/P$ is not reduced. Conversely, if we have some nilpotent element $Q \in K[X]/P$ then we have $P|Q^k$ for some $k \geq 2$ but $P \not| Q$. The only way that this is possible is if P has a root of multiplicity greater than 1.

4. From class, we have the formula

$$\operatorname{disc}(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_{L/K}(P'(\alpha)),$$

where α is a root of the monic irreducible polynimial P and $L = K(\alpha)$. Since P is irreducible, $\operatorname{Hom}_K(L, \bar{K})$ acts transitively on the roots of P. We thus have

$$\begin{aligned} \operatorname{disc}(1, \alpha, \ldots, \alpha^{n-1}) &= (-1)^{\frac{n(n-1)}{2}} N_{L/K}(P'(\alpha)) \\ &= (-1)^{\frac{n(n-1)}{2}} \prod_{\sigma \in \operatorname{Hom}_K(L, \bar{K})} \sigma(P'(\alpha)) \\ &= (-1)^{\frac{n(n-1)}{2}} \prod_{1 \leq i \leq n} \sigma(P'(\alpha_i)), \end{aligned}$$

where $\alpha_1, \ldots, \alpha_n \in \bar{K}$ are the roots of P. Thus, we have

$$\operatorname{disc}(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{\frac{n(n-1)}{2}} \operatorname{Res}(P', P)$$

by 2c and the fact that P is monic.

5. Let K be a number field and O_K its ring of integers. Suppose that $O_K = \mathbf{Z}[\alpha]$ for some $\alpha \in O_K$, and that Q is the minimal polynomial of α (of degree n). In this case, we have from a result in class that $\operatorname{disc}(K) = \operatorname{disc}(1, \alpha, \ldots, \alpha^n) = \pm D(P)$ by the previous item. Let p be any prime. Then we know that $\mathbf{Z}[X]/(p, Q) = (\mathbf{Z}/p)[X]/Q = (\mathbf{Z}[X]/Q)/p = O_K/pO_K$. Since $\mathbf{Z}/p = \mathbf{F}_p$ is perfect, we have that $(\mathbf{Z}/p)[X]/Q$ is reduced iff $D(P) \neq 0$ in $\mathbf{F}_p$. That is, iff $p \not| D(P)$. Hence, O_K/p is reduced iff $p \not| \operatorname{disc}(K)$.

2 A Special Case of Kronecker-Weber

For any positive integer m, set $\zeta_m = e^{2\pi i/m}$. Let p be an odd prime. From class, we know that $\operatorname{disc}(\zeta_p) = \pm p^{p-2}$ is a square in $\mathbf{Q}(\zeta_p)$. Since p is odd, this implies that $p - 2$ is odd and hence that $\mathbf{Q}(\sqrt{\pm p}) \subset \mathbf{Q}(\zeta_p)$. It is obvious that $\mathbf{Q}(i) = \mathbf{Q}(\zeta_4)$, and that $Q(\zeta_8) \supset \mathbf{Q}(\sqrt{2})$, since $\zeta_8 + \zeta_8^7 = \sqrt{2}$. Thus, for any prime p (even or odd), $\mathbf{Q}(\sqrt{p}) \subset \mathbf{Q}(\zeta_{4p})$. This follows for $p = 2$ by the above, and for odd p since $\mathbf{Q}(\zeta_{4p}) \supset \mathbf{Q}(\zeta_p, \zeta_4) = \mathbf{Q}(\sqrt{\pm p})(i) \supset \mathbf{Q}(\sqrt{p})$. We now show that for any m, $\mathbf{Q}(\sqrt{m})$ is contained in some cyclotomic field. Without loss of generality, assume that m is square free. Then we may write $m = p_1 p_2 \cdots p_k$ for distinct primes p_i. We have $\mathbf{Q}(\sqrt{m}) \subset \mathbf{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_n})$. However, we have shown that $\mathbf{Q}(\sqrt{p_i}) \subset \mathbf{Q}(\zeta_{4p_i}) \subset \mathbf{Q}(\zeta_{4p_1 \cdots p_n})$, since $\zeta_{4p_1 \cdots p_n}^{p_1 \cdots \hat{p_i} \cdots p_n} = \zeta_{4p_i}$, where $\hat{p_i}$ denotes that p_i is omitted from the product. Thus, every quadratic extension of $\mathbf{Q}$ is contained in some cyclotomic field.

3 Stickelberger's Criterion

Let K be a number field of degree n over $\mathbf{Q}$ and fix algebraic integers $\alpha_1, \ldots, \alpha_n$. Let $\sigma_1, \ldots, \sigma_n$ denote the n embeddings of K in $\mathbf{C}$. We can write $d = \operatorname{disc}(\alpha_1, \ldots, \alpha_n) = |\sigma_i(\alpha_j)|^2 = (P - N)^2$, where P denotes the product

$$\sum_{\tau \in A_n} \prod_{i=1}^{n} \sigma_i(\alpha_{\tau(i)}),$$

and N is given by

$$\sum_{\tau \in S_n \setminus A_n} \prod_{i=1}^{n} \sigma_i(\alpha_{\tau(i)}),$$

that is, P is the sum in the determinant corresponding to even permutations, while N corresponds to the odd permutations. Notice that since the α_i are algebraic integers, $\sigma_j(\alpha_i)$ are algebraic integers also (since any σ_j must sent any α_i to a root of its minimal polynomial), and since the set of all algebraic integers forms a ring, P, N must also be algebraic integers. Now, let L be some normal closure of K in $\mathbf{C}$ with $\operatorname{Gal}(L/\mathbf{Q}) = \{\sigma_1, \ldots, \sigma_n\}$. Now the σ_j act on the set $\{1, \ldots, n\}$ by defining $\tilde{\sigma_j}(k)$ to be the integer l such that $\sigma_j \sigma_k = \sigma_l$. Thus, clearly, $\tilde{\sigma_j} \in S_n$ for each j. Now, for any *even* $\tilde{\sigma}$, we have

$$\begin{aligned}
\sigma(P) &= \sum_{\tau \in A_n} \prod_{i=1}^{n} \sigma\sigma_i(\alpha_{\tau(i)}) \\
&= \sum_{\tau \in A_n} \prod_{i=1}^{n} \sigma_i(\alpha_{\tau\tilde{\sigma}^{-1}(i)}) \\
&= P
\end{aligned}$$

upon reindexing. Similarly, we have for any even $\tilde{\sigma}$ that $\sigma(N) = N$, while for odd $\tilde{\sigma}$ we have $\sigma(P) = N$ and $\sigma(N) = P$. Since every element of $\operatorname{Gal}(L/\mathbf{Q})$ is either even or odd, we find that

$$\begin{aligned}
N + P&, \\
NP&,
\end{aligned}$$

are both fixed by every embedding σ_j, (and hence every element of Gal$(L/\mathbf{Q})$ and hence must be in $\mathbf{Q}$. Since they are algebraic integers in $\mathbf{Q}$, they must be in $\mathbf{Z}$. Hence, $d = (P-N)^2 = (P+N)^2 - 4PN$ is congruent to 1 or 0 modulo 4.

4 Ring of Integers of Biquadratic Extensions

1. (a) One direction is easy: if $\alpha \in R$ then the relative norm and trace over $\mathbf{Q}(\sqrt{m})$ are algebraic integers. This follows from the fact that the norm and trace are, respectively, a product and sum of embeddings of $K = \mathbf{Q}[\sqrt{m}, \sqrt{n}]$ in $\mathbf{C}$ over $\mathbf{Q}[\sqrt{m}]$, since any such embedding sends α to a root of its minimal polynomial, and the fact that R is a ring. Conversely, let us suppose that the norm and trace, $a = N^K_{\mathbf{Q}[\sqrt{m}]}(\alpha)$, $b = T^K_{\mathbf{Q}[\sqrt{m}]}(\alpha)$, are algebraic integers. Clearly $K/\mathbf{Q}[\sqrt{m}]$ is galois since it is a degree two extension. Let σ generate the galois group. Then since $a = \alpha\sigma(\alpha)$, $b = \alpha+\sigma(\alpha)$, we find that α is a root of $P(X) = X^2 - bX + a$. We know that a, b are algebraic integers, and since they are fixed by σ, they must be elements of $\mathbf{Q}[\sqrt{m}]$, so that $P \in \mathbf{Q}[\sqrt{m}][X]$. Now let τ generate Gal$(\mathbf{Q}[\sqrt{m}]/\mathbf{Q})$. Then $Q = P\tau(P)$ is a degree 4 polynomial with coefficients in $\mathbf{Q}$ that has α as a root. In fact, Q is clearly monic since P is, and the coefficients of Q are algebraic integers since a, b are. Thus, Q is a monic polynomial in $\mathbf{Z}[X]$ with α as a root, showing that α is an algebraic integer.

2. (b) We write $\alpha = p + q\sqrt{m} + r\sqrt{n} + s\sqrt{k}$ and consider the three relative traces, $t_1 = T^K_{\mathbf{Q}[\sqrt{m}]}(\alpha)$, $t_2 = T^K_{\mathbf{Q}[\sqrt{n}]}(\alpha)$, $t_3 = T^K_{\mathbf{Q}[\sqrt{k}]}(\alpha)$. By part (a), α is an algebraic integer iff t_1, t_2, t_3 are. Let σ_1, σ_2, $sigma_3$ generate Gal$(K/\mathbf{Q}[\sqrt{m}])$, Gal$(K/\mathbf{Q}[\sqrt{n}])$, Gal$(K/\mathbf{Q}[\sqrt{k}])$ respectively. It is not difficult to see that each σ_i reverses the sign on two of the radicals and preserves the signs on the constant term and the third radical in our expression for α. Thus we obtain $t_1 = 2p + 2q\sqrt{m}$, $t_2 = 2p + 2r\sqrt{n}$, $t_3 = 2p + 2s\sqrt{k}$. Since no one of m, n, k is congruent to 1 modulo 4, we must have $2p$, $2q$, $2r$, $2s$ all integers. From this we conclude that we may write

$$\alpha = \frac{a + b\sqrt{m} + c\sqrt{n} + d\sqrt{k}}{2}$$

for some a, b, c, $d \in \mathbf{Z}$. Now consider $N = N^K_{\mathbf{Q}[\sqrt{m}]}(\alpha)$. We have just as above

$$\begin{aligned} N &= \frac{a + b\sqrt{m} + c\sqrt{n} + d\sqrt{k}}{2} \frac{a + b\sqrt{m} - c\sqrt{n} - d\sqrt{k}}{2} \\ &= \frac{(a^2 + mb^2 - nc^2 - kd^2) + 2(ab - cdn/(m,n))\sqrt{m}}{4}. \end{aligned}$$

Now n is even and m is odd so that $2|cdn/(m,n)$, from which we must have $2|ab$. (Of course, since N must be an algebraic integer.) Hence one of $a,\ b$ is even. But again, $n,\ k$ are even, so $2|(a^2+mb^2)$, and since 4 divides one of $a^2,\ b^2$, we conclude that 2 must divide the other, so that in fact, both $a,\ b$ are even. Now $4|(a^2+mb^2)$ so that $4|(nc^2+kd^2)$ If $c,\ d$ have opposite parity, then one of $c^2,\ d^2$ is 0 modulo 4 and the other is 1 modulo 4, so that, since $n,\ k$ are 2 modulo 4, nc^2+kd^2 is 2 modulo 4, a contradiction. Hence, $c,\ d$ have the same parity. From this, we conclude that an integral basis for R is

$$\left\{1, \sqrt{m}, \sqrt{n}, \frac{\sqrt{n}+\sqrt{k}}{2}\right\}.$$

3. (f) Since we know an integral basis for R, it is not hard to compute $\mathrm{disc}(R)$. we have

$$\begin{aligned}
\mathrm{disc}(R) &= |\sigma_i(\alpha_j)|^2 \\
&= \begin{vmatrix} 1 & \sqrt{m} & \sqrt{n} & \frac{\sqrt{n}+\sqrt{k}}{2} \\ 1 & -\sqrt{m} & \sqrt{n} & \frac{\sqrt{n}-\sqrt{k}}{2} \\ 1 & \sqrt{m} & -\sqrt{n} & \frac{-\sqrt{n}-\sqrt{k}}{2} \\ 1 & -\sqrt{m} & -\sqrt{n} & \frac{-\sqrt{n}+\sqrt{k}}{2} \end{vmatrix}^2 \\
&= 64mnk
\end{aligned}$$

where we have expanded about the first column using Cramer's Rule.