Math 129 HW 6

Bryden Cais

March 31, 2002

1 Multiplicities in the Discriminant

20) Suppose that the elements $\alpha_{ij}\beta$ for $1 \leq i \leq r$, $1 \leq j \leq e_i$ and $\beta \in B_i$ are linearly dependent over R/P. That is, we have a relation

$$\sum_{i=1}^{r}\sum_{j=1}^{e_i}\sum_{\beta\in B_i} c_{ij\beta}\alpha_{ij}\beta \equiv 0 \mod P, \tag{1}$$

where $c_{ij\beta} \in R/P$. From the definition of α_{ij} as an element in the ideal $(Q_i^{j-1} - Q_i^j) \cap (\bigcap_{h\neq i} Q_h^{e_h})$, we readily see that $Q_i^k|\alpha_{ij}$ for all $j > k$ and $Q_i^k|\alpha_{lj}$ for all $l \neq i$ and any j as long as $k \leq e_i$. Therefore, considering 1 modulo Q_i for each i we see that

$$\sum_{\beta\in B_i} c_{i1\beta}\alpha_{i1}\beta \equiv 0 \mod Q_i$$

for each i. Since B_i is a set of coset representatives for a basis of S/Q_i and $\alpha_{i1} \not\equiv 0 \mod Q_i$, we must have $c_{i1\beta} \equiv 0 \mod Q_i$ for all i and all β. Now suppose that we have $c_{ik\beta} \equiv 0 \mod Q_i$ for all i and β. Then consider 1 module Q_i^{k+1}. We then obtain

$$\sum_{j=1}^{k+1}\sum_{\beta\in B_i} c_{ij\beta}\alpha_{ij}\beta \; equiv 0 \mod Q_i^{k+1}.$$

Since $c_{ij\beta} \equiv 0 \mod Q_i$ for all i, β and $j \leq k$, we then see that

$$\sum_{\beta\in B_i} c_{i(k+1)\beta}\alpha_{i(k+1)}\beta \equiv 0 \mod Q_i,$$

which implies, as before, that $c_{i(k+1)\beta} \equiv 0 \mod Q_i$ for all i and all β. By induction, then we have that $c_{ij\beta} \equiv 0 \mod Q_i$ for all $1 \le i \le r$, $1 \le j \le e_i$ and all $\beta \in B_i$. Viewing the $c_{ij\beta}$ as elements of R (that is, picking representatives of the P cosets in R) we see that $c_{ij\beta} \in (Q_i)$ for each i. Since $c_{ij\beta} \in R$, we have $c_{ij\beta} \in R \cap Q_i$, that is, $c_{ij\beta} \in (P)$. This holds for each i, j, β, so that $c_{ij\beta} = 0$ in R/P for all i, j, β, which shows that the $\alpha_{ij}\beta$ are linearly independent over R/P.

21) Suppose that $p||S/G|$ where G is the free abelian group generated by $\alpha_1, \dots, \alpha_n$. Then S/G contains an element of order p, say β with $p\beta \equiv 0 \mod G$. That is, $p\beta \in G$ so that we have $p\beta = x_1\alpha_1 + cdots + x_n\alpha_n$ with $x_n \in \mathbf{Z}$. We therefore have $x_1\alpha_1 + cdots + x_n\alpha_n \equiv 0 \mod p$ so that $x_i \equiv 0 \mod p$ for all i since the α_i are independent mod p. We therefore have $x_i = py_i$ for some $y_i \in \mathbf{Z}$ so that $\beta = y_1\alpha_1 + \cdots + y_n\alpha_n$ is in G whence $\beta = 0$ in S/G and does not have order p, a contradiction. Hence, $p \not| |S/G|$. Since exercise 27 of chapter 2 tells us that $\operatorname{disc}(\alpha_1, \dots, \alpha_n) = |S/G|^2 \operatorname{disc}(S)$, we have that $\operatorname{disc}(\alpha_1, \dots, \alpha_n) = m \operatorname{disc}(S)$ with $p \not| m$.

Now let $\alpha_1, \dots, \alpha_n$ be the set constructed in exercise 20. We know that this set is independent mod p. From the definition of this set, we readily see that a given prime Q over p divides exactly $k = \sum_{j=1}^r (e_j - 1) f_j$ of the α_i. We have shown that if $\sigma : K \longrightarrow \mathbf{C}$ is any imbedding then $\sigma^{-1}(Q)$ is also a prime over p and therefore divides α_i for k values of i, so that $Q|\sigma(\alpha_i)$ for k values of i. Therefore, if $\{\sigma_1, \dots, \sigma_s\}$ are the imbeddings of K into $\mathbf{C}$, we see that for every j, we have $Q|\sigma_j(\alpha_i)$ for exactly k values of i. Since $\operatorname{disc}(\alpha_1, \dots, \alpha_n)$ is the determinant $|\sigma_j(\alpha_i)|$, we see that Q^k divides $\operatorname{disc}(\alpha_1, \dots, \alpha_n)$. Since the discriminant is in $\mathbf{Z}$, we have that $Q^k \cap \mathbf{Z} = p^k$ divides $\operatorname{disc}(\alpha_1, \dots, \alpha_n)$. Therefore, since $\operatorname{disc}(\alpha_1, \dots, \alpha_n) = m \operatorname{disc}(S)$ with $p \not| m$, we see that $p^k | \operatorname{disc}(S)$.

28) Since α is a root of $x^n + a_{n-1}x^{n-1} + \cdots + a_0$ with $p^r | a_j$ for all j, we see that

$$\begin{aligned} \alpha^n &= p^r \left(-\frac{a_{n-1}}{p^r}\alpha^{n-1} - \cdots - \frac{a_0}{p^r} \right) \\ &:= p^r \beta, \end{aligned}$$

with $\beta \in R$. Since $p^{r+1} \not| a_0$, we see that (β) and (p^r) are relatively prime.

Now write $(\alpha) = Q_1^{e_1} \cdots Q_t^{e_t}$ uniquely as a product of prime ideals. Then we have $\prod_{i=1}^t Q_i^{ne_i} = (p^r)(\beta)$. Since (β) and (p^r) are relatively prime, for each i we have $Q_i^{ne_i}$ dividing (p^r) or (β). Let $i_1, \dots, i_k$ be those i for which $Q_i^{ne_i}$ divides (p^r). Then we must have $Q_j^{ne_j}$ dividing (β) for any j which is not one of the i_l. Since in fact $(\alpha^n) = (p^r)(\beta)$, we must have

$$\begin{aligned} p^r &= Q_{i_1}^{ne_{i_1}} \cdots Q_{i_1}^{ne_{i_k}} \\ &= (Q_{i_1}^{e_{i_1}} \cdots Q_{i_1}^{e_{i_k}})^n, \end{aligned}$$

so that p^r is the n^{th} power of some ideal in R.

Now suppose that $(n,r)=1$. Since $(p^r)=I^n$ for some ideal I, we may decompose both sides into their unique prime factorizations to obtain

$$P_1^{re_1}\cdots P_s^{re_s} \;=\; Q_1^{nf_1}\cdots Q_t^{nf_t}$$

from which we obtain $s=t$ and, renumbering if necessary, $re_i=nf_i$ for each i. Therefore, $n|re_i$ and since $(n,r)=1$ we conclude that $n|e_i$ so that we may write $e_i=n\epsilon_i$ and hence

$$p=(P_1^{\epsilon_1}\cdots P_s^{\epsilon_s})^n.$$

Therefore, p is the n^{th} power of some ideal, $p=Q^n$. Since the primes π_i above p satisfy

$$\sum_{i=1}^{d} f(\pi_i|p)e(\pi_i|p)=n \tag{2}$$

we see that p only has one prime above and that p is totally ramified. That is, $d=1, f=1$ and $e=n$.

By exercise 21, we see that $p^k=p^{n-\sum_{i=1}^{d}(f_i)}=p^{n-1}$ divides disc(R). In the case that $(n,r)=m>1$, we may show, just as above, that $p=(Q)^{n/m}$ for some ideal Q and therefore that the ramification indices of the primes above p are all divisible by n/m. Write $e_i=m_i(n/m)$ and use formula 2 to obtain

$$\sum_{i=1}^{d} f_i \le \sum_{i=1}^{d} m_i f_i = \sum_{i=1}^{d} e_i\frac{m}{n}f_i=m,$$

and hence $n-\sum_{i=1}^{d}\ge n-m$, from which (by exercise 21 again) it follows that $p^{n-m}|\operatorname{disc}(R)$.

2 Totally Ramified Primes

24) Let $K\subset M\subset L$ be field extensions and suppose that a prime $p\in K$ is totally ramified in L. There is only one prime, say Q above p in L. Since there is a unique prime below Q in M, we see that there is only one prime above p in M, say π. We also know that $f(Q|\pi)f(\pi|p)=f(Q|p)=1$, so that $f(\pi|p)=1$ also. Therefore, since $f(\pi|p)e(\pi|p)=e(\pi|p)=[M:K]$, we conclude that p is totally ramified in M.

Now suppose that L,L' are field extensions of K and that p is totally ramified in L and unramified in L'. Let $M=L\cap L'$. Then we know that p is totally ramified in M since $M\subset L$ is a subfield. Therefore, let π be the unique prime above p in M. We then have $\pi^m=p$ where $m=[M:K]$. Now suppose that π factors in L' as $\pi=Q_1^{e_1}\cdots Q_s^{e_s}$. Then we have the factorization $p=Q_1^{me_1}\cdots Q_s^{me_s}$ in L'. Since p is unramified in L', we must have $me_i=1$ for all i and therefore $m=1$ whence $M=K$.

3 Completely Split Primes

30) Let f be any nonconstant polynomial over $\mathbf{Z}$. We show that f has a root modulo p for infinitely many primes p. First assume that $f(0) = 1$. We then have $f(n!) \equiv 1 \mod n!$ for any n. THerefore, the prime divisors of $f(n!)$ are greater than or equal to n, from which we deduce that there are infinitely many primes p for which f has a root modulo p. If $f(0) = 0$ then obviously f has a root modulo every prime p since it has a root in $\mathbf{Z}$, so we may suppose that $f(0) \neq 0$. Now there are only finitely many primes dividing $f(0)$, so excluding them from our considerations, we see that iff $f(0) \neq 1$ then $g(x) = f(xf(0))/f(0)$ is well defined modulo p and satisfies $g(0) = 1$. Notice that any root of g yields a root of f. We are therefore reduced to the previous case.

Now let $K = \mathbf{Q}(\alpha)$ be a number field with $g \in \mathbf{Z}[X]$ the minimal polynomial of α. Suppose that g factors modulo p as $\bar{g_1}^{e_1} \cdots \bar{g_r}^{e_r}$. From [1, pg. 79] we know that if $p \in \mathbf{Z}$ does not divide $|S/\mathbf{Z}[\alpha]|$ then the prime decomposition of p in K is given by

$$Q_1^{e_1} \cdots Q_r^{e_r},$$

where $Q_i^{e_i} = (p, g_i(\alpha))$ and $f(Q_i|p) = deg(g_i)$. Since there are infinitely many primes p for which the polynomial g has a root modulo p, we see that there are infinitely many primes p for which g has a linear factor and hence for which there is a prime Q over p with $f(Q|p) = 1$.

Let K, L be number fields with $K \subset L$. Denote by $\bar{L}$ the normal closure of L over K. We know that there are infinitely many primes $P_{\bar{L}}$ of $\bar{L}$ with $f(P_{\bar{L}}|P_{\mathbf{Z}}) = 1$ where $P_{\mathbf{Z}}$ is the unique prime in $\mathbf{Z}$ below $P_{\bar{L}}$. Since $\bar{L}/K$ is Galois, we have the relation $efd = [\bar{L} : \mathbf{Q}]$ where $e = e(P_{\bar{L}}|P_{\mathbf{Z}})$, $f = f(P_{\bar{L}}|P_{\mathbf{Z}}) = 1$, and d is the number of primes over $P_{\mathbf{Z}}$ in $\bar{L}$. Since only finitely many primes of $\mathbf{Z}$ are ramified in $\bar{L}$, we see that there are infinitely many primes $P_{\bar{L}}$ such that the unique prime $P_{\mathbf{Z}}$ below splits into $[\bar{L} : \mathbf{Q}]$ factors in $\bar{L}$, i.e. splits completely in $\bar{L}$. Let P_K be the unique prime below $P_{\bar{L}}$ in K. Then using the relations

$$\begin{aligned} f(P_{\bar{L}}|P_L)f(P_L|P_L)f(P_K|P_{\mathbf{Z}}) &= f(P_{\bar{L}}|P_{\mathbf{Z}}) = 1 \\ e(P_{\bar{L}}|P_L)e(P_L|P_K)e(P_K|P_{\mathbf{Z}}) &= e(P_{\bar{L}}|P_{\mathbf{Z}}) = 1, \end{aligned}$$

we see that $e(P_L|P_K) = f(P_L|P_K) = 1$ for infinitely many primes $P_{\bar{L}}$. Since there are only finitely many primes in $\bar{L}$ above any given prime in K, we see that there must be infinitely many primes P_K of K which split completely in L.

Let f be a nonconstant monic irreducible polynomial over a number ring $R \subset K$ and let α be a root of f. Set $L = K(\alpha)$. By Theorem 27 [1, pg. 79], we know that if $f = \bar{g_1}^{e_1} \cdots \bar{g_r}^{e_r}$ mod P where the $\bar{g_i}$ are irreducible modulo P then the prime factorization of P in L is given by $P = Q_1^{e_1} \cdots Q_r^{r_r}$, where $Q_i = (P, g_i(\alpha))$ and $f(Q_i|P) = deg(g_i)$. We have shown that there are infinitely many primes P of R which split completely in L, and therefore infinitely many

P for which all the g_i have degree one, that is, for which f splits into linear factors modulo P.

4 Splitting Primes in Biquadratic Extensions

6) Let m, n be distinct, squarefree integers and set $K = \mathbf{Q}(\sqrt{m}, \sqrt{n})$. Then K contains three quadratic subfields, $\mathbf{Q}(\sqrt{m}), \mathbf{Q}(\sqrt{k}), \mathbf{Q}(\sqrt{k})$, where $k = mn/(m,n)^2$. Let p be a prime in $\mathbf{Z}$. In any examples that follow, we shall make implicit use of the following trivial calculation:

$$\begin{aligned}
\operatorname{disc}(\sqrt{m}+\sqrt{n}) &= N\left(4(\sqrt{m}+\sqrt{n})((\sqrt{m}+\sqrt{n})^2-(m+n))\right) \\
&= 2^{12}m^2n^2(m-n)^2 \\
&= \operatorname{Index}(\sqrt{m}+\sqrt{n})\operatorname{disc}(R) \\
&= 2^b\operatorname{Index}(\sqrt{m}+\sqrt{n})\frac{m^2n^2}{(m,n)^2},
\end{aligned}$$

where $b = 0, 4$ or 6, depending on the residues of $m, n \mod 4$. In this manner, we may determine whether or not a given prime divides $\operatorname{Index}(\sqrt{m}+\sqrt{n})$, and therefore whether or not Theorem 27 [1, pg. 79] is applicable.

Suppose that p is ramified in each of the quadratic subfields. Then we know that p divides the discriminant of each of these fields. But we know that the discriminant of $\mathbf{Q}(\sqrt{d})$ is d or $4d$ depending on whether $d \equiv 1 \mod 4$ or $d \not\equiv 1 \mod 4$. Therefore, if p is a prime other than 2, it must divide m, n, and k. But the definition of k shows that this is impossible, so that $p = 2$. Observe that $\alpha = \sqrt{m}+\sqrt{n}$ is of degree 4 over $\mathbf{Q}$, so that it therefore generates the extension $K/\mathbf{Q}$. The minimal polynomial of α over $\mathbf{Z}$ is easily seen to be

$$f(X) = (X^2-(m+n))^2 - 4mn.$$

Reducing modulo 2 and using the fact that $X^2-1 \equiv (X-1)^2 \mod 2$, we see that $f(X) \equiv X^4 \mod 2$ if $m+n$ is even and $f(X) \equiv (X-1)^4 \mod 2$ is $m+n$ is odd. In any case, the prime p (that is, 2) is totally ramified in K. As an example, we let $m = 3$, $n = 6$, $k = 2$. Then we have the ideal factorizations

$$\begin{aligned}
2 &= (2, 1+\sqrt{3})^2 \\
2 &= (2, 2+\sqrt{6})^2 \\
2 &= (\sqrt{2})^2
\end{aligned}$$

so that 2 is totally ramified in each quadratic subfield. We also easily have

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

in K.

We know that K is just the composite of $\mathbf{Q}(\sqrt{m})$ and $\mathbf{Q}(\sqrt{n})$. By Theorem 31 [1, pg. 107], if a prime P splits completely in $\mathbf{Q}(\sqrt{m})$ and $\mathbf{Q}(\sqrt{n})$ then it splits completely in their composite. Thus, P must split completely. As an example, we take $m = 2$, $n = 15$, and $p = 7$. Then since $1, 2$ are squares modulo 7 we see that 7 splits in $\mathbf{Q}(\sqrt{m})$ and $\mathbf{Q}(\sqrt{n})$. In fact,

$$\begin{aligned}
7 &= (7, \sqrt{2}+3)(7, \sqrt{2}-3) && \text{in } \mathbf{Q}(\sqrt{2}),\\
7 &= (7, \sqrt{15}+1)(7, \sqrt{15}-1) && \text{in } \mathbf{Q}(\sqrt{15}),\\
7 &= (7, \sqrt{30}+3)(7, \sqrt{30}-3) && \text{in } \mathbf{Q}(\sqrt{30}),\\
7 &= (7, \sqrt{15}+\sqrt{2}-2)(7, \sqrt{15}+\sqrt{2}+2)(7, \sqrt{15}+\sqrt{2}-3)(7, \sqrt{15}+\sqrt{2}+3) && \text{in } K.
\end{aligned}$$

Notice that P cannot be inert in each of the quadratic subfields. To see this, we observe that P is inert in $\mathbf{Q}(\sqrt{m})$ if and only if $x^2 - m$ is irreducible modulo P. That is, if and only if

$$\left(\frac{m}{P}\right) = -1,$$

where $\left(\frac{m}{P}\right)$ is the Jacobi symbol of $m \mod P$. But since $k = mn/(m,n)^2$, we easily see that

$$\left(\frac{k}{P}\right) = \left(\frac{m}{P}\right)\left(\frac{n}{P}\right),$$

so that if P is inert in $\mathbf{Q}(\sqrt{m})$ and $\mathbf{Q}(\sqrt{n})$, then m, n are not squares modulo P and therefore k *is* a square modulo P so that P is *not* inert in $\mathbf{Q}(\sqrt{k})$.

Let $m = 3, n = 2$ and $p = 3$. The minimal polynomial of $\sqrt{2}+\sqrt{3}$ is $(X^2-5)^2 - 24 \equiv (X^2+1)^2 \mod 3$. Since X^2+1 is irreducible modulo 3, we find that the factorization of 3 in $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ is

$$3 = (3, 2\sqrt{6})^2.$$

Now let m, n be as above but consider $p = 5$. We have [1, pg. 79] that $(X^2-5)^2 - 24 \equiv X^4 + 1 \equiv (X^2+2)(X^2-2) \mod 5$. Since $(X^2 \pm 2)$ are irreducible modulo 5 we find that 5 splits as

$$5 = (5, 2+2\sqrt{6})(5, 3+2\sqrt{6})$$

in $\mathbf{Q}(\sqrt{2}, \sqrt{3})$.

Finally, let $m = 5, n = 6$, and $p = 5$. Then since the minimal polynomial of $\sqrt{5} + \sqrt{6}$ is $(X^2 - 11)^2 - 120 \equiv (X - 1)^2(X + 1)^2 \mod 5$, we see that 5 factors as

$$5 = (5, \sqrt{5} + \sqrt{6} + 1)^2(5, \sqrt{5} + \sqrt{6} - 1)^2$$

in $\mathbf{Q}(\sqrt{5}, \sqrt{6})$.

7) Let $K = \mathbf{Q}(\sqrt{-1})$ and $L = \mathbf{Q}(\sqrt{-5})$. We show that 2 is totally ramified in K, L, but not in KL. It is not difficult to see that we have the factorizations

$$\begin{aligned} 2 &= (1 + \sqrt{-1})^2 \quad \text{in } K \text{ and} \\ 2 &= (2, 1 + \sqrt{-5})^2 \quad \text{in } L. \end{aligned}$$

On the other hand,

$$2 = \left(2, \frac{1}{2}(-1 + \sqrt{-1})(1 + \sqrt{5})\right)^2,$$

as you will check (with tears). That this is a prime ideal follows from the fact that $\frac{1}{2}(-1 + \sqrt{-1})(1 + \sqrt{5})$ has norm 4. We note that this gives an example of a prime (2) that totally ramifies in K and L but not in KL and of a prime that gives trivial residue field extensions for K, L, but not for KL. Of course, both of these phenomena are unusual and happen because 2 divides Index$(\sqrt{-1} + \sqrt{-5})$.

Now consider $K = \mathbf{Q}(\sqrt{3}), L = \mathbf{Q}(\sqrt{3})$, and $p = 7$. It is clear that 7 is inert in K, L since $3, 5$ are quadratic non residues modulo 7. However, 7 factors in KL as

$$7 = (7, 3 + 2\sqrt{15})(7, 2 + 2\sqrt{15}),$$

which is readily checked. This therefore gives an example where a prime 7 has unique primes lying over it in K, L (namely 7) but not in KL. It also gives an example of a prime that is inert in K, L but not in KL. That covers all the examples required in the problem.

References

[1] Marcus, D.A. *Number Fields*. Springer Verlag, New York. 1977.