Math 129, Test 1

Bryden Cais

March 18, 2002

1 The Prime Divisors of Index(K)

1. Let $q = p^r$ and let α be a root of a degree r monic irreducible polynomial in $\mathbf{F}_p[X]$. Then $\mathbf{F}_p[\alpha]$ is a degree r extension of $\mathbf{F}_p$ and is therefore isomorphic to $\mathbf{F}_q$. We therefore have a surjective map $\mathbf{Z}[\alpha] \longrightarrow \mathbf{F}_q$, which shows that F_q is primitive.

2. In one direction, suppose $A = \mathbf{Z}[\alpha]$ is primitive and that $A = k_1 \times k_2 \times \cdots \times k_m$ is a product of finite fields. Write $\alpha = (\alpha_1, \ldots, \alpha_m)$ with $\alpha_j \in k_j$ for each j. Certainly, $\mathbf{Z}[\alpha_j] = k_j$ for each j. Notice that for any polynomial f we have $f(\alpha) = (f(\alpha_1), \ldots, f(\alpha_m))$. Therefore, since $(1, \ldots, 1, 0, 1, \ldots, 1) \in A = \mathbf{Z}[\alpha]$, where the 0 is in the i th position, we have some polynomial $f \in \mathbf{F}_p[X]$ such that $f(\alpha_j) = \delta_{ij}$. Thus, $\mathrm{Irred}(\alpha_i)|f$ and $\mathrm{Irred}(\alpha_j) \not| f$ for $i \neq j$. Hence, we have distinct monic irreducible polynomials $P_i, \ldots, P_m \in \mathbf{F}_p[X]$ with $\deg(P_i) = f_i = [k_i : \mathbf{F}_p]$ since $k_i = \mathbf{Z}[\alpha_i]$.

   In the other direction, suppose that $P_i, \ldots, P_m \in \mathbf{F}_p[X]$ with $\deg(P_i) = f_i = [k_i : \mathbf{F}_p]$ are such polynomials. Then let α_i be a root of P_i in some splitting field and set

   $$\alpha = (\alpha_1, \ldots, \alpha_m).$$

   Let R_i be the polynomial in $\mathbf{F}_p[X]$ given by $P_1 \cdots \hat{P_i} \cdots P_m$, where the hat indicates omission. Define $\beta_i = R_i(\alpha_i)$, and set $B_i = \mathrm{Irred}(\beta_i)$. Clearly, $\beta_i \neq 0$, so that $B_i(0) \neq 0$ since B_i is irreducible and $\deg(B_i) \geq 1$. Now let

   $$Q_i(X) = \frac{-X}{B_i(0)}(B_i(R_i(X)) - B_i(0)).$$

   It is not difficult to see that $Q_i(X) \in \mathbf{F}_p[X]$ and $Q_i(\alpha) = (0, \ldots, 0, \alpha_i, 0, \ldots, 0)$. Since $\mathbf{Z}[\alpha_i] = k_i$, we have shown that $A = \mathbf{Z}[\alpha]$ is primitive.

3. One direction is trivial: Since $I^e \subset I$, we have $R/I^e \supset R/I$, so that if R/I^e is primitive, R/I is also. Now suppose that R/I is primitive and that

$$I \;=\; P_1^{r_1} P_2^{r_2} \cdots P_m^{r_m}$$

for distinct prime ideals P_j and integers $r_j > 0$. By the chinese remainder theorem, we then have

$$R/I^e \;=\; R/P_1^{er_1} \times R/P_2^{er_2} \times \cdots \times R/P_m^{er_m},$$

4. Let $I = I_1 \cdots I_m$ with $N(I_j) = p_j^{f_j}$ for distinct p_j. Then the ideals I_i, I_j are relatively prime for $i \neq j$. In other words, the chinese remainder theorem applies and gives

$$R/I \simeq R/I_i \times \cdots \times R/I_m.$$

Clearly, if R/I is primitive, then R/I_i is primitive for every i. We already proved this in item 1. (Notice the proof in this direction works even without the hypothesis that all of the factors be finite fields.) Assume now that R/I_i is primitive for each i, say $R/I_i \simeq \mathbf{Z}[\alpha_i]$. Let $g_i \in \mathbf{Z}[X]$ be the irreducible polynomial of α_i. Then we have $R/I_i \simeq \mathbf{Z}[X]/g_i(X)$. We then apply the chinese remainder theorem again to give

$$R/I \simeq \mathbf{Z}[X]/g_1 \cdots g_m.$$

Now let α be the image of X in R/I under the above isomorphism. Clearly, then, α generates R/I and hence R/I is primitive.

5. Using the unique decomposition of I into prime ideals, we write $I = I_1 \cdots I_m$ where $N(I_i)$ is a power of p_i and the p_i are distinct primes. By item 4, R/I is primitive if and only if R/I_i is primitive for all i. We factor I_i into a product of prime ideals as $I_i = P_1^{e_1} \cdots P_m^{e_m}$, for distinct prime ideals P_j. Notice that every prime ideal $P \supset I$ of norm a power of p_i is one of the P_j.

   Notice that our proof for item 4 does not only uses the fact thatI_i, I_j are relatively prime for $i \neq j$. Therefore, since the P_j are distinct, they are all relatively prime so that R/I_i is primitive if and only if $R/P_j^{e_j}$ is primitive for each j. By item 3, this is the case if and only if R/P_j is primitive for each j, that is, again by 4, if and only if

$$R/P_1 P_2 \cdots P_m$$

   is primitive. Now we are in the situation of item 2, and we see that this quotient is primitive if and only if there exist distinct monic irreducible polynomials $g_j \in \mathbf{F}_{p_i}[X]$

with $\deg(g_j) = f_j$ where $f_j = R/P_j = N(P_j)$. (since all the P_j have norm a power of p_i, and therefore the quotient is a product of finite fields of characteristic p_i).

If the number of prime ideals containing I of norm p_i^f is greater than the number of irreducible monic polynomials of degree f in $\mathbf{F}_p[X]$, we see that there cannot possibly be the distinct polynomials as in item 2, so that R/I_i is not primitive. Conversely, if there are at least as many distinct irreducible polynomials of degree f as there are prime ideals containing I_i of norm p_i^f, then $R/P_1 \times \cdots \times R/P_m$ is primitive, and hence R/I_i is primitive. Following the chain of reasoning backwards, we see that this completes the proof.

6. In one direction, suppose that the $P_1, \ldots, P_m$ are prime ideals each with norm p^f and that m is strictly greater than the number of irreducible monic polynomials of degree f in $\mathbf{F}_p[X]$. Let $I = P_1 \cdots P_m$. Then item 5 tells us that R/I is not primitive. Since $N(I)$ is a power of p, $\#R/I$ and hence $\#(R/I)/\mathbf{Z}[\alpha]$ is a power of p also. Since R/I is not primitive, $\#(R/I)/\mathbf{Z}[\alpha]$ is a nontrivial power of p for any α. This implies that $p | \#R/\mathbf{Z}[\alpha]$ for any α, and hence $p | \operatorname{Index}(K)$.

2 A Nice Ring

1. To show commutativity, notice that as d ranges over all divisors of n, so does n/d, so that we may reindex the sum defining $f * g$ to obtain

$$\begin{aligned} (f * g)(n) &= \sum_{d|n} f(d)g(n/d) \\ &= \sum_{d|n} f(n/d)g(d) \\ &= (g * f)(n). \end{aligned}$$

Associativity of $*$ is proved similarly. We have

$$\begin{aligned} (f * (g * h))(n) &= \sum_{d|n} \sum_{d'|(n/d)} f(d)g(d'h(n/dd')) \\ &= \sum_{\delta|n} \sum_{d|\delta} f(d)g(\delta/d)h(n/d) \\ &= ((f * g) * h)(n) \end{aligned}$$

upon replacing dd' by δ and reindexing the sum. Let

$$e(n) = \begin{cases} 1 & \text{if} \quad n = 1 \\ 0 & \text{otherwise} \end{cases}.$$

Then we obviously have $(f * e)(n) = f(n)$ for all n and any $f \in \mathcal{L}$, so that e is the identity element. We finally have to check some trivial properties, for example that

$$\begin{aligned} (f + g) * h &= f * h + g * h \quad \text{and} \\ f * \lambda \cdot g &= \lambda \cdot f * g, \end{aligned}$$

which follow from

$$\begin{aligned} \sum_{d|n} (f(d) + g(d)) h(n/d) &= \sum_{d|n} f(d) h(n/d) + \sum_{d|n} g(d) h(n/d), \\ \sum_{d|n} f(d) \lambda g(n/d) &= \lambda \sum_{d|n} f(d) g(n/d). \end{aligned}$$

Now if $f \in \mathcal{L}$ and $f(1) = 0$ then $(f * g)(1) = f(1)g(1) = 0$ no matter what g is, so that f is not invertable. Conversely, if $f(1) \neq 0$, then we may define $f^{-1}(1) = 1/f(1)$, and we can define $f^{-1}(n)$ for $n > 1$ inductively as

$$f^{-1}(n) = -\frac{1}{f(1)} \sum_{\substack{d|n \\ d<n}} f^{-1}(d) f(n/d). \tag{1}$$

It is then not difficult to see that $f * f^{-1} = e$. Finally, suppose that $f * g \equiv 0$. Suppose that $g \not\equiv 0$. Let m be the least integer for which $g(m) \neq 0$. Then since $(f * g)(m) = 0$, we have

$$0 = \sum_{d|m} f(d) g(m/d) = f(1) g(m),$$

so that $f(1) = 0$. Now we show by induction that $f \equiv 0$. Suppose that $f(d) = 0$ for all $d < k$. Since $(f * g)(mk) = 0$, we have

$$\begin{aligned} 0 &= \sum_{d|mk} f(d) g(n/d) \\ &= \sum_{\substack{d|mk \\ d<k}} f(d) g(mk/d) + \sum_{\substack{d|mk \\ d>k}} f(d) g(mk/d) + g(m) f(k) \\ &= g(m) f(k), \end{aligned}$$

since $f(d) = 0$ for $d < k$ and $g(mk/d) = 0$ for $d > k$ because we chose m to be the least integer for which $g(m)$ was nonzero. Thus, we have $f(k) = 0$ and by induction, $f \equiv 0$ as claimed.

2. We show that $f * g$ is multiplicitive if $f,\ g$ are. Let $(m, n) = 1$. Then any d with $d|mn$ may be written *uniquely* as $d = d_1 d_2$ where $d_1|m$ and $d_2|n$. We need only take $d_1 = (m, d)$ and $d_2 = (n, d)$. Thus there is a bijection between divisors d of mn and pairs (d_1, d_2) with $d_1|m$, $d_2|n$ and $d_1 d_2 = d$. (Since the other direction is clear). Therefore, we have

$$\sum_{d|mn} f(d)g(mn/d) \ = \ \sum_{d_1|m}\sum_{d_2|n} f(d_1 d_2)g(mn/d_1 d_2). \tag{2}$$

Again, since $(m, n) = 1$, we have $(d_1, d_2) = (m/d_1, m/d_2) = 1$ for any $d_1|m$ and $d_2|n$. Thus, since f, g are multiplicative, we find

$$\begin{aligned}
\sum_{d|mn} f(d)g(mn/d) \ &= \ \sum_{d_1|m}\sum_{d_2|n} f(d_1)f(d_2)g(m/d_1)g(n/d_2) && (3)\\
&= \ \sum_{d_1|m} f(d_1)g(m/d_1)\sum_{d_2|n} f(d_2)g(n/d_2) && (4)\\
&= \ (f * g)(m)(f * g)(n). && (5)
\end{aligned}$$

Since $(f * g)(1) = f(1)g(1) = 1$, $f * g$ is multiplicative. Obviously, e is multiplicitive. We may use our definition 1 to show by induction that f^{-1} is also multiplicitive. Since $f(1) = 1$, we have $f^{-1}(1) = 1$. Now suppose that for all $m, n < N$, we have $f^{-1}(mn) = f^{-1}(m)f^{-1}(n)$ whenever $(m, n) = 1$. Then

$$\begin{aligned}
f^{-1}(mN) \ &= \ -\frac{1}{f(1)}\sum_{\substack{d|m\\ d<m}}\sum_{d'|N} f^{-1}(dd')f(mN/dd')\\
&\quad -\frac{f^{-1}(m)}{f(1)}\sum_{\substack{d'|N\\ d'<N}} f^{-1}(d')f(N/d')\\
&= \ f^{-1}(m)f^{-1}(N),
\end{aligned}$$

where we have used the same summation reindexing techniques as in 2, and 3 and the assumption that $(m, N) = 1$. This shows, in fact, that f^{-1} is multiplicitive for all $(m, n) \leq N$ with $(m, n) = 1$, so by induction, f^{-1} is multiplicitive. Obviously, if f, g

are multiplicitive, then $f \times g$ is also multiplicitive since we have $f(1)g(1) = 1$ and

$$\begin{aligned}(f \times g)(mn) &= f(mn)g(mn) = f(m)f(n)g(m)g(n) \\ &= (f(n)g(n))(f(m)g(m)) = (f \times g)(n)(f \times g)(m).\end{aligned}$$

This shows that the set of multiplicitive functions is a subgroup of $\mathcal{L}^*$ which is stable under $\times$.

3. Define z by $z(n) = 1$ for all n, and let μ be the inverse of z under $*$. First, we clearly have $\mu(1) \cdot 1 = 1$ so that $\mu(1) = 1$. Now for any prime p, we must have $\mu(p) + \mu(1) = 0$ so that $\mu(p) = -1$ for all primes. We also have

$$\mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^r) = 0$$

for any $r \geq 2$ so that

$$\mu(p^2) + \cdots + \mu(p^r) = 0$$

for any $r \geq 2$ whence by induction, $\mu(p^r) = 0$ for all $r \geq 2$. Since z is multiplicitive and μ is its inverse, μ is also multiplicitive. Thus we have completely determined the behavior of μ and have

$$\mu(n) = \begin{cases} 1 & \text{if} \quad n = 1 \\ 0 & \text{if} \quad n \text{ has a square factor} \\ (-1)^k & \text{if} \quad n = p_1 p_2 \cdots p_k \end{cases}$$

where all the p_j are distinct. We note an interesting consequence: Let

$$f(n) = (z * g)(n) = \sum_{d|n} g(d).$$

Then

$$(\mu * f)(n) = (\mu * z * g)(n) = (e * g)(n) = g(n).$$

The converse is also clear.

4. Let $\varphi(n)$ be Euler's phi function and let $i(n) = n$ for all n. We know that φ is multiplicitive, so that $\varphi * z$ is also multiplicitive. Moreover,

$$\begin{aligned}\sum_{d|p^r} \varphi(d) &= \sum_{i=1}^{r} \varphi(p^i) \\ &= \sum_{i=1}^{r} \left(p^i - p^{i-1}\right) \\ &= p^r.\end{aligned}$$

Therefore, decomposing any integer as a product of primes and applying the above, we have, by the multiplicitivity of $\varphi * z$ that $(\varphi * z)(n) = n$ for any n.

5. We have

$$z * z \;=\; \sum_{d|n} 1,$$

which obviously counts the number of divisors of n. Similarly,

$$i * z \;=\; \sum_{d|n} d,$$

which clearly gives the sum of the divisors of n.

6. Now suppose that f is completely multiplicitive. The fact that $\times f$ is a $\mathbf{C}$-algebra homomorphism of $(\mathcal{L}, +, *, \cdot)$ will follow if we can show that it preserves the multiplicitive $*$ structure of $\mathcal{L}$, as the other requirements are trivial to check. We have

$$\begin{aligned}(f \times g) * (f \times h)(n) &= \sum_{d|n} f(d)g(d)f(n/d)h(n/d) \\ &= f(n) \sum_{d|n} g(d)h(n/d) \\ &= f \times (g * h)(n)\end{aligned}$$

for all n. We also have

$$\begin{aligned}f * (\mu \times f) &= \sum_{d|n} f(d)\mu(n/d)f(n/d) \\ &= f(n) \sum_{d|n} \mu(n/d) \\ &= f(n)\mu * z \\ &= f(n)e(n) \\ &= e(n)\end{aligned}$$

since $f(1) = 1$. Here we have used the fact that μ is the inverse under $*$ for z. This shows that $\mu \times f$ is the inverse under $*$ of f.

3 Irreducible Polynomials Over $\mathbf{F}_q$

1. This is not difficult. For irreducible polynomials of degree $1, 2, 3$ it is enough to check for polynomials that do not have a root in $\mathbf{F}_p$. For degree 4 polynomials, we need only exclude polynomials that have a root in $\mathbf{F}_p$ and polynomials that are the product of two irreducible quadratics. Thus, we find

$$\begin{aligned}
I_2(1) &= \{x, x+1\} \\
I_2(2) &= \{x^2+x+1\} \\
I_2(3) &= \{x^3+x^2+1, x^3+x+1\} \\
I_2(4) &= \{x^4+x+1, x^4+x^3+1, x^4+x^3+x^2+x+1\}
\end{aligned}$$

$$\begin{aligned}
I_3(1) &= \{x, x+1, x+2\} \\
I_3(2) &= \{x^2+1, x^2+x+2, x^2+2x+2\} \\
I_3(3) &= \left\{\begin{matrix} x^3+2x+1, x^3+2x+2, x^3+x^2+2, x^3+x^2+x+2, \\ x^3+x^2+2x+1, x^3+2x^2+1, x^3+2x^2+x+1, x^3+2x^2+2x+2 \end{matrix}\right\}
\end{aligned}$$

$$\begin{aligned}
I_5(1) &= \{x, x+1, x+2, x+3, x+4\} \\
I_5(2) &= \left\{\begin{matrix} x^2+x+1, x^2+x+2, x^2+2x+3, x^2+2x+4, \\ x^2+3x+3, x^2+3x+4, x^2+4x+1, x^2+4x+2 \end{matrix}\right\}.
\end{aligned}$$

2. We first prove that

$$x^{q^m} - x \quad \text{divides} \quad x^{q^n} - x$$

if and only if $m|n$. First suppose that $m|n$, say $n = ms$. We employ the identity

$$y^d - 1 = (y-1)(y^{d-1} + y^{d-2} + \cdots + 1) \tag{6}$$

with $y = q^m$ and $d = s$ to find that $q^m - 1 | q^n - 1$. Now set $y = x^{q^m - 1}$ and $d = (q^n - 1)/(q^m - 1)$ in 6 to see that $x^{q^m} - x$ divides $x^{q^n} - x$, as claimed. Conversely, if $m \not| n$ then $a = q^n$ is not a power of $b = q^m$, so $\mathbf{F}_a$ is not an extension of $\mathbf{F}_b$. But since the elements of $\mathbf{F}_a$ are precisely the roots of $x^a - x$, we see that $x^b - x$ cannot divide $x^a - x$.

Now let $P \in I_q(d)$. Let α be a root of P in some extension of $\mathbf{F}_q$. Then the field $K = \mathbf{F}_q(\alpha)$ has degree d over $\mathbf{F}_q$ and its elements are the roots of $x^{q^d} - x$. Since α is thus a root of $x^{q^d} - x$ and P is irreducible, $P | x^{q^d} - x$, and hence by the above, $P | x^{q^r} - x$

for all r divisible by d. Conversely, if $P|x^{q^n}-x$ for some n, then the field generated by a root of P must be a subfield of $\mathbf{F}_{q^n}$. As above, this implies that q^n is some power of q^d, that is, $d|n$.

3. By the previous item, we see that the irreducible polynomials of degree d in $\mathbf{F}_q[x]$ are precisely the degree d irreducible factors of $X^{q^n}-x$ when $d|n$, and hence we may write

$$x^{q^n}-x \;=\; \prod_{d|n}\prod_{P\in I_q(d)} P.$$

Counting degrees now gives

$$\sum_{d|n} dr_q(d) \;=\; q^n. \tag{7}$$

4. Notice that we may rewrite 7 in the form

$$(i\times r_q)*z \;=\; q^n.$$

We may apply 6 to the above identity to obtain

$$\begin{aligned}(i\times r_q)*z*\mu &= \mu*q^n\\ &= (i\times r_q)*e\\ &= (i\times r_q),\end{aligned}$$

or what is the same thing,

$$r_q(n) \;=\; \frac{1}{n}\sum_{d|n}\mu(n/d)q^d.$$

5. From our formula for the möbius function, we have

$$nr_q(n) \;\geq\; q^n-(q+q^2+\cdots+q^{n-1}) \;=\; q^n-\frac{q^n-q}{q-1}.$$

Now using the fact that, for $n\geq 1$ we always have

$$q^n\geq q,$$

we see that

$$q^n(q-2)\geq q(q-2),$$

with equality only if $q = 2$ or $n = 1$. We expand this inequality and rearrange terms to obtain

$$\frac{q^{n+1} - 2q^n + q}{q - 1} \geq q,$$

that is,

$$q^n - \frac{q^n - q}{q - 1} \geq q,$$

so that

$$nr_q(n) \ \geq \ q,$$

with equality only possible when $q = 2$ or $n = 1$. It is clear that equality always holds when $n = 1$ since the ploynomial $x + r$ is irreducible for every $r \in \mathbf{F}_q$. The possibility of equality when $q = 2$ may be ruled out as we are only summing over the divisors of a particular integer m and not over all $k \leq m$. (Moreover, the möbius function is not always negative one). In any case, it is easy to see that for $n \neq 1$ and $q = 2$, we have grossly underestimated things and equality above holds if and only if $n = 1$.

4 A Bound for $p|\operatorname{Index}(K)$

1. Suppose that $p|\operatorname{Index}(K)$. Then item 6 of section 1 tells us that for some f, the number of monic irreducible polynomials of degree f in $\mathbf{F}_p[X]$ is strictly less than the number of prime ideals $P_1, \ldots, P_m$ of norm p^f. Then $m > r_p(f)$. By item 5 of section 3, we have

$$m > r_p(f) \geq \frac{p}{f},$$

or $mf > p$. Since $[K : \mathbf{Q}] = n$, we have $[R : \mathbf{Z}] = n$ and therefore $[R : \mathbf{Z}[\alpha]] \leq n$ for any α. Notice that $R/P_1 \cdots P_m$ is an $\mathbf{F}_p$ vector space of dimension mf. Since $\mathbf{F}_p$ is primitive, we write $\mathbf{F}_p = \mathbf{Z}[\alpha]$ for some alpha. Then we see that R may be considered (with the same sense of equality as above) as an $\mathbf{F}_p$ vector space of dimension at most n. Since R contains $R/P_1 \cdots P_m$, comparing dimensions gives $n \geq mf$, and therefore $n > p$.

2. Let $K = \mathbf{Q}(\sqrt{7}, \sqrt{10})$. Supose that $\mathcal{O}_K = \mathbf{Z}(\alpha)$ for some α and let f be the monic irreducible polynomial for α over $\mathbf{Z}$. We will denote by $\bar{g}$ the reduction modulo 3 of the polynomial $g \in \mathbf{Z}[X]$.

(a) We know that $g(\alpha)$ is divisible by 3 in $\mathbf{Z}[\alpha]$ if and only if g is zero in $\mathbf{Z}[\alpha]/3 = \mathbf{Z}[X]/(f,3) = \mathbf{Z}_3[X]/\bar{f}$, that is, if and only if $\bar{f}$ divides $\bar{g}$ in $\mathbf{Z}_3[X]$.

(b) Let $\alpha_i = (1+(-1)^{\lfloor\frac{i-1}{2}\rfloor}\sqrt{7})(1+(-1)^{i-1}\sqrt{10})$, for $1 \le i \le 4$. Clearly, the products $\alpha_i\alpha_j$ for $i \neq j$ are each divisile by one of $N(1+\sqrt{7}) = -6$, $N(1+\sqrt{10}) - 9$ in $\mathbf{Z}[\alpha]$. Thus, in any case, $\alpha_i\alpha_j$ is divisible by 3 in $\mathbf{Z}[\alpha]$ for $i \neq j$. Obviously, the four embeddings of K into $\mathbf{C}$ send each α_i to the four α_j. Thus,

$$Tr(\alpha_i^n) \;=\; \alpha_1^n + \alpha_2^n + \alpha_3^n + \alpha_4^n.$$

Since all of the cross terms $\alpha_i^k\alpha_j^m$ with $i \neq j$, $m, k > 0$ are divisible by 3 in $\mathbf{Z}[\alpha]$, we have

$$Tr(\alpha_i^n) \equiv (\alpha_1+\alpha_2+\alpha_3+\alpha_4)^n = 4^n \mod 3$$

in $\mathbf{Z}[\alpha]$. However, since the trace is an integer, this congruence holds in $\mathbf{Z}$. Therefore, $Tr(\alpha_i^n) \equiv 1 \mod 3$ in $\mathbf{Z}$, so it is not divisible by 3. Hence, α_i^n is not divisible by 3 in $\mathbf{Z}[\alpha]$ for any n.

(c) Since we are supposing that $\mathbf{Z}[\alpha] = \mathcal{O}_K$, let $\alpha_i = f_i(\alpha)$ for each i. Then by part a, we see that $\bar{f} | \bar{f}_i\bar{f}_j$ in $\mathbf{Z}_3[X]$ for $i \neq j$ but $\bar{f} \not| \bar{f}_i^n$ for any n. Therefore, since $\mathbf{Z}_3[X]$ is a UFD, f has an irreducible factor which does not divide $\bar{f}_i$ but does divide all f_j for $i \neq j$.

(d) This shows that f has at least 4 distinct irreducible factors over $\mathbf{F}_3[X]$. Since f has degree at most 4, we conclude that f splits completely into 4 distinct linear factors over $\mathbf{F}_3$. But there are only 3 distinct linear irreducible factors (up to units, of course) in $\mathbf{F}_3[X]$ and this is a contradiction. Thus, $\mathcal{O}_K \neq \mathbf{Z}[\alpha]$ for any α. That is, $R = \mathcal{O}_K$ is not primitive. This shows that Index$(\alpha) > 1$ for any α. Now we showed on an earlier homework (Marcus, ex. 42) that an integral basis for R is

$$\left\{1, \sqrt{7}, \sqrt{10}, \frac{\sqrt{10}+\sqrt{70}}{2}\right\}$$

and that disc(K) is $2^8 \cdot 5^2 \cdot 7^2$. Using the previous item, we see that if $p|$ Index(K) then $p < 4$, so that $p = 2$ or 3. We can rule out $p = 2$ because $\mathbf{Q}((\sqrt{10}+\sqrt{70})/2) = K$ since the former is of degree 4 and contained in K, but disc$((\sqrt{10}+\sqrt{70})/2) = 2^8 \cdot 3^2 \cdot 5^6 \cdot 7^2$, and therefore Index$((\sqrt{10}+\sqrt{70})/2) = 75$. Thus, Index$(K) = 3$. Incidentally, one may compute a polynomial as in section 5 item 5:

$$P(X,Y,Z) \;=\; (2X^2 - 5Z^2)(2Y^2 + 2YZ - 3Z^2)(14X^2 - 5(2Y+Z)^2).$$

5 The Second Question

1. From class, (or Marcus pg. 36) we have the following result: Suppose that K is a number field and R its ring of integers. Let $\alpha \in R$ and suppose that α has degree n over $\mathbf{Q}$. Then there is an integral basis

$$1, \frac{f_i(\alpha)}{r_1}, \ldots, \frac{f_{n-1}(\alpha)}{d_{n-1}}$$

where f_i has degree i and $d_1|d_1|\ldots|d_{n-1}$, the d_i are uniquely determined, and

$$\text{disc}(\alpha) = (d_1 d_2 \cdots d_{n-1})^2 \text{disc}(R).$$

Therefore, R has an integral basis of the form $1 = \omega_1, \omega_2, \ldots, \omega_n$.

2. Let $\alpha = \sqrt[3]{175}$. The irreducible polynomial of α is $X^3 - 175$, form which we easily compute $\text{disc}(\alpha) = -3^3 \cdot 5^4 \cdot 7^2$. Now it can be shown (Marcus pg. 49) that in the above notation, $d_1^6|\text{disc}(\alpha)$. Therefore we conclude that $d_1 = 1$. Notice that $\alpha^2/5 = 5^{1/3} \cdot 7^{2/3}$ is integral. Therefore, $5|d_2$. Again, from our discriminant computation, we see that $d_2|3 \cdot 5^2 \cdot 7$. Set $f_2(\alpha) = \alpha^2 + a\alpha + b$. If $7|d_2$ then $f_2(\alpha)/7$ is integral (from the theorem). We see then by considering the trace of this element that $7|b$ since $Tr(\alpha) = (1 + \omega + \omega^2)\alpha = 0$. Therefore, $(\alpha^2 + a\alpha)/7$ is integral. We then cube this element and consider its trace, using the fact that the trace of α is 0. We obtain $Tr((\alpha^2 + a\alpha)^3/7^3) = 525(175 + a^3)/7^3$. Therefore, $7|a^3$, from which we see that $7|a$ and that $\alpha^2/7$ is integral. But this is false, so that $7 \not| d_2$. Now suppose that $25|d_2$. Again, $(\alpha^2 + a\alpha + b)/25$ is integral so that by considering the trace, we see that $25|b$ and that $5^6|525(175 + a^3)$, and hence $5|a$ so that $5|7$, a contradiction. Thus, $25 \not| d_2$. We finally show that $3 \not| d_2$. Squaring $f_2(\alpha)/d_2$ shows that

$$\frac{(a^2 + 2b)\alpha^2 + (2ab + 175)\alpha + (b^2 + 350a)}{d_2^2}$$

is integral. Therefore, since we can write this in terms of α and $f_2(\alpha)/d_2$, we must have that d_2 divides each of $(a^2 + 2b), (2ab + 175), (b^2 + 350a)$. If $3|d_2$ then these equations imply that $a \equiv b \equiv 1 \mod 3$. Therefore, $(\alpha - 1)^2/3 = (\alpha^2 - 2\alpha + 1)/3 \in R$. Raising this element to the fourth power and considering its trace implies that $3^4|3^3 \cdot 131 \cdot 719$, which is a contradiction. Therefore, $3 \not| d_2$ and $d_2 = 5$. Thus, we have an integral basis for R:

$$\left\{1, 175^{1/3}, \frac{175^{2/3}}{5}\right\}.$$

3. This is trivial: Since $x_1 \in \mathbf{Z}$ and $\omega_1 = 1$, we see that $\mathbf{Z}[\alpha] = \mathbf{Z}[\alpha - x_1]$ and therefore $\mathrm{Index}(\alpha) = \#R/\mathbf{Z}[\alpha] = \#R/\mathbf{Z}[\alpha - x_1] = \mathrm{Index}(\alpha - x_1)$.

4. We will use the equation $\mathrm{disc}(\alpha) = \mathrm{Index}(\alpha)^2\mathrm{disc}(K)$ and the fact that $\mathrm{disc}(\alpha) = |\sigma_i(\alpha_j)|^2$ where σ_i are the distinct imbedings of K into $\mathbf{C}$ and $\alpha_j = \alpha^j$. Set

$$\alpha = x_1\omega_1 + \cdots + x_n\omega_n.$$

Then $\mathrm{Index}(\alpha) = \mathrm{Index}(\alpha - x_1)$ by the previous item. Clearly,

$$\begin{vmatrix} 1 & \sigma_1(\alpha) & \cdots & \sigma_1(\alpha^{n-1}) \\ \vdots & & & \vdots \\ 1 & \sigma_n(\alpha) & \cdots & \sigma_n(\alpha^{n-1}) \end{vmatrix}$$

is a polynomial in $x_1, x_2, \ldots x_n$ with integral coefficients in a quadratic extension of $\mathbf{Q}$ (since any automorphism at worst flips the sign of this determinant). Moreover, this polynomial, call it $Q(x_2, \ldots, x_n)$ satisfies $Q/\sqrt{\mathrm{disc}(K)} = \mathrm{Index}(\alpha)$. Since $\mathrm{disc}(K)$ is an integer, and since $\mathrm{Index}(\alpha)$ is an integer for every α, we conclude that $P = Q/\sqrt{\mathrm{disc}(K)}$ is a polynomial in $x_2, \ldots, x_n$ with coefficients in some degree 2 or 4 extension of $\mathbf{Q}$ that takes only integer values. Therefore, $P \in \mathbf{Z}[x_1, \ldots, x_n]$.

5. We now compute such a polynomial for $K = \mathbf{Q}(175^{1/3})$. We write

$$\beta \;=\; \alpha - x_1 \;=\; Xa + Ya^2/5,$$

for any $\alpha \in R$ with $a = 175^{1/3}$. We readily compute

$$\beta^2 \;=\; X^2a^2 + 7y^2a + 70XY.$$

The two nontrivial imbeddings of K into $\mathbf{C}$ are given by $\sigma_2(a) = \omega a$ and $\sigma_3(a) = \omega^2 a$, where ω is a cube root of unity. Therefore, we must calculate the determinant

$$\begin{vmatrix} 1 & Xa + Ya^2/5 & X^2a^2 + 7y^2a + 70XY \\ 1 & X\omega a + Y\omega^2a^2/5 & X^2\omega^2a^2 + 7y^2\omega a + 70XY \\ 1 & X\omega^2 a + Y\omega a^2/5 & X^2\omega a^2 + 7y^2\omega^2 a + 70XY \end{vmatrix}$$

This is somewhat tedious, but we find that the determinant is equal to

$$-105\sqrt{-3}(5X^3 - 7Y^3).$$

It remains to divide this polynomial by $\sqrt{\mathrm{disc}(K)}$. Using the integral basis found above, we readily compute

$$\begin{aligned} \sqrt{\mathrm{disc}(K)} &= \begin{vmatrix} 1 & a & a^2/5 \\ 1 & \omega a & \omega^2 a^2/5 \\ 1 & \omega^2 a & \omega a^2/5 \end{vmatrix} \\ &= -105\sqrt{-3}. \end{aligned}$$

Therefore, we have

$$P(X,Y) = 5X^3 - 7Y^3.$$

From this it follows that $\mathrm{Index}(K) = 1$ since $(5,7) = 1$. If R were primitive, we could find some $X, Y \in \mathbf{Z}$ such that $5X^3 - 7Y^3 = 1$. We view this equation modulo 7 so see that we have a solution to $X^3 \equiv 3 \mod 7$. The cubes modulo 7 are $1, -1,$, so that this is impossible and R is not primitive.