Math 129, Test 1

Bryden Cais

March 11, 2002

1 The Prime Divisors of $\mathrm{Index}(K)$

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 $\mathrm{Irred}_j \not| f$ 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 $P_1 \cdots \hat{P_i} \cdots \mathbf{P}1_m$, 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.

We now claim that this result holds even if we only know that

$$A = D_1 \times D_2 \times \cdots \times D_m$$

with each $D_j = R/Q_j^{r_j}$ for some prime ideal Q_j and nonzero r_j. To see that this is true, notice that we only use that the k_i are fields in our proof when we divide by $B_i(0)$, and otherwise we do not use that the k_i are of the same characteristic or even integral domains. So all that we must show to prove this extension is that $B_i(0)$ is always a unit. Notice, however, that since R is a number ring, $R/Q_j^{r_j}$ is always principal, so that Bezout's theorem applies. That is, with P_i as before, since the P_i are distinct irreducible polynomials, there exist polynomials a, b such that

$$aP_i + bP_j = 1$$

for $i \neq j$. Evaluation at α_i (a root of P_i) gives $b(\alpha_i)P_j(\alpha_i) = 1$, so that $P_j(\alpha_i)$ is a unit for each $j \neq i$. Therefore, β_i is also a unit since it is a product of units. It follows that all galois conjugates of β_i are units, and therefore also that $N(\beta_i) = B_i(0)$ is a unit, as required.

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 $g(1) \not\equiv 0$. 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* $d = d_1 d_2$ 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

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

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

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

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

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

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 $p|\,\mathrm{Index}(K)$

1.