Notes for Number Theory in Function Fields - Rosen

Henry T. & Drake T.

August 1, 2019

The following is a non-comprehensive list of side notes for Rosens's *Number Theory in Function Fields*. The hope is that this PDF makes reading the text more smooth. Page notes appear here in the order that you will come across them on the page when reading the text. Diagrams will be included when necessary.

§1 Polynomials over Finite Fields

Page 3

- > . . . From the above considerations we have
  >
  > $$(A/fA)^* \cong (A/P_1^{e_1}A)^* \times (A/P_2^{e_2}A)^* \times \cdots \times (A/P_t^{e_t}A)^*$$

  The reason why α in $f = \alpha P_1^{e_1} P_2^{e_2} \cdots P_t^{e_t}$ doesn't appear in the isomorphism is because it's invertible in A. So we could include it in one of the quotients but it won't change anything up to isomorphism.

Page 4

- > . . . The ring A/P^eA has only one maximal ideal PA/P^eA which has $|P|^{e-1}$ elements. Thus $(A/P^eA)^* = A/P^eA - PA/P^eA$ . . .

  Maximality follows from the fourth isomorphism theorem for rings since PA is maximal in A, order follows from looking at what a full set of representatives looks like just remember to pull out the factor of P, and uniqueness is because the maximal ideal in A, under the fourth isomorphism theorem correspondence, must contain $P^e A$. Since this maximal ideal is unique, the quotient ring is local which means this maximal ideal contains all non-units implying $(A/P^e A)^* = A/P^e A - PA/P^e A$.

- > . . . So we have a group of order $|P|$ with exponent p . . .

  What this means by definition is that the least common multiple of all orders of elements in the group is p.

- > . . . $(A/P^2A)^{(1)}$ is a direct sum of $f \deg(P)$ number of copies of $\mathbb{Z}/p\mathbb{Z}$. This is cyclic under the very restrictive conditions that $q = p$ and $\deg(P) = 1$ . . .

  We can make this identification as follows. Recall that every element of $(A/P^2A)^{(1)}$ is represented by $1 + bP$ for $b \in A$. By the Euclidean algorithm, $b = qP + r$ for some polynomial $r \in P$ with $\deg(r) \leq P$. Then $bP = qP^2 + rP$ and since we are working modulo P^2A we may take our representative to be $1+rP$. As b ranges over all polynomials, r ranges over all polynomials of degree at most $p - 1$. Since $1 + rP$ only depends on r we may identify $1 + rp$ as an element of p copies of $\mathbb{Z}/q\mathbb{Z}$ using the coefficients of r. Since $q = p^f$, $\mathbb{Z}/q\mathbb{Z}$ is isomorphic to f copies of $\mathbb{Z}/p\mathbb{Z}$. These two facts together give the identification of $(A/P^2A)^{(1)}$ with $f \deg(P)$ copies of $\mathbb{Z}/p\mathbb{Z}$. The statement regarding when $(A/P^2A)^{(1)}$ is cyclic follows since the direct sum of two cyclic groups $\mathbb{Z}/m\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ is cyclic if and only if $(n, m) = 1$.

Page 5

- > . . . Such an r represents a unit in A/fA if and only if it is relatively prime to f . . .

  To see this, recall that

  $$(A/fA)^* \cong (A/P_1^{e_1}A)^* \times (A/P_2^{e_2}A)^* \times \cdots \times (A/P_t^{e_t}A)^*.$$

  Now by Proposition 1.6 an element is in $(A/P_i^{e_i}A)^*$ if and only if its an element of $(A/P_i^{e_i}A) - (P_iA/P_i^{e_i}A)$. So if r represents a unit in A/fA, then r determines a class in $(A/P_i^{e_i}A) - (P_iA/P_i^{e_i}A)$ which means r is of the form $a + P_i^{e_i}a'$, $a, a' \in A$, where a is not a multiple of P_i and therefore neither is r. Since this happens for all i, r must be relatively prime to f. Conversely, if r is relatively prime to f, then r determines a class in $(A/P_i^{e_i}A)$ for all i and can't be of the form $P_ia + P_i^{e_i}a'$ for otherwise it shares a common factor P_i with f. Via the isomorphism this implies r represents a unit in A/fA.

Page 6

- > …where the bars denote cosets modulo P …

  Technically we mean the ideal generated by P, namely PA.

- > …Since there are $|P| - 1$ roots and the difference of the two sides has degree less than $|P| - 1$, the difference of the two sides must be 0 …

  We are using the polynomial identity trick here.

Page 7

- > …Suppose $f = \alpha P_1^{e_1} P_2^{e_2} \cdots P_t^{e_t}$ is the prime decomposition of f. Then it is easy to check that a is a d-th power residue modulo f if and only if a is a d-th power residue modulo $P_i^{e_i}$ for all i between 1 and t …

  This easy check is accomplished by the Chinese Remainder Theorem since we have a solution modulo f if and only if we have solutions modulo $P_i^{e_i}$ for all i.

- > …If $b^d \equiv a \pmod{P}$, then $a^{\frac{|P|-1}{d}} \equiv b^{|P|-1} \equiv 1 \pmod{P}$ by the corollary to Proposition 1.8 …

  Indeed, b is relatively prime to P. Otherwise, it's congruent to 0 modulo P which implies a is also congruent to 0 modulo P, or in other words, P divides a. This is contradictory to the assumption.

- > …there are $\frac{|P|-1}{d}$ d-th powers in $(A/PA)^*$ …

  Let φ be the d-th power map. Since the image is the d-th powers, by the first isomorphism theorem the number of d-th powers is $|(A/PA)^*|/|\ker\varphi| = \frac{|P|-1}{d}$.

- > …The natural map (i.e., reduction modulo P) is a homomorphism from $(A/P^eA)^*$ onto $(A/PA)^*$ and the kernel is a p-group as follows from Proposition 1.6. Since the order of $(A/PA)^*$ is $|P|-1$ which is prime to p it follows that $(A/P^eA)^*$ is the direct product of a p-group and a copy of $(A/PA)^*$ …

  We give some more detail as to why $(A/P^eA)^*$ is the direct product of a p-group, say K, and a copy of $(A/PA)^*$. First notice that by the first isomorphism theorem we have

$$(A/P^eA)^*/K \cong (A/PA)^*.$$

By Lagrange, $|(A/P^eA)^*| = p^n(|P|-1)$ for some $n \geq 1$ since a finite group is a p-group if and only if its order is p^n for some $n \geq 1$. Now p does not divide $|P|-1$ so K is a Sylow p-subgroup. Since $(A/P^eA)^*$ is a finite abelian group it must be isomorphic to a direct product of its Sylow p-subgroups. Hence $(A/P^eA)^*/K$ is isomorphic to the direct product of all the Sylow p-subgroups of $(A/P^eA)^*$ except K. This implies

$$(A/P^eA)^* \cong ((A/P^eA)^*/K) \oplus K \cong (A/PA)^* \oplus K,$$

which is the desired isomorphism.

§2 Primes, Arithmetic Functions, and The Zeta Function

Page 11

- > . . . so one has
  >
  > $$\sum_{\deg(f)\leq d} |f|^{-s} = 1 + \frac{q}{q^s} + \frac{q^2}{q^{2s}} + \cdots + \frac{q^d}{q^{ds}},$$
  >
  > and consequently
  >
  > $$\zeta_A(s) = \frac{1}{1-q^{1-s}}$$

  In the sum above we also assume each f is monic. To see how to get from the sum to the fractional expression for $\zeta_A(s)$, take the limit as d tends to infinity to get an infinite geometric series. Its sum is the expression for $\zeta_A(s)$.

Page 13

- > . . . taking the logarithmic derivative of both sides and multiplying the result by u yields
  >
  > $$\frac{qu}{1-qu} = \sum_{d=1}^{\infty} \frac{da_d u^d}{1-u^d}.$$
  >
  > Finally, expand both sides into power series using the geometric series and compare coefficients of u^n . . .

  The logarithmic derivative of a function f is defined to be f'/f. Its easy to show that if $f = gh$, then $f'/f = (g'/g) + (h'/h)$ so that products are turned into sums. This is what is used to get the identity above. Now expanding the left-hand side is easy. For the right-hand side, expand $1/(1-u^d)$ and write the series as a double series. Then notice that we have terms $da_d u^n$ precisely when d divides n.

Page 14

- > …The total number of terms is $\sum_{d|n} |\mu(d)|$, which is easily seen to be 2^t …

  The d-th term is 0 if it contains the square of a prime. So, we can construct each nonzero d-th term by choosing to either include or exclude every distinct prime factor of n. There are clearly 2^t choices, and the value of each term is 1 by the definition of the absolute value of the Mobius function.

- > …Thus we have the following estimate:
  >
  > $$\left|a_n - \frac{q^n}{n}\right| \leq \frac{q^{\frac{n}{2}}}{n} + q^{\frac{n}{3}}$$

  We can see this in the following way: a_n is at least larger than q^n/n because that is the highest power of q appearing in a_n (note that $\mu(1) = 1$). So, the inside of the left-hand side is positive and we get the absolute values for free because the negative of the right-hand side is less than zero. Disregarding the absolute value, the left-hand side counts all the remaining terms past the first. There is a possible $q^{\frac{n}{2}}/n$ term if 2 divides n so we include it on the right-hand side because we want an upper bound. Then the remaining terms are at most $q^{\frac{n}{3}}/n$ and we have at most 2^t of them, but $2^t < n$ so we upper bound by $n(q^{\frac{n}{3}}/n) = q^{\frac{n}{3}}$.

- > …Then,
  >
  > $$a_n = \frac{q^n}{n} + O\left(\frac{q^{\frac{n}{2}}}{n}\right)$$

  If this is not clear, drop the absolute value in

  $$\left|a_n - \frac{q^n}{n}\right| \leq \frac{q^{\frac{n}{2}}}{n} + q^{\frac{n}{3}},$$

  factor out $q^{\frac{n}{2}}/n$ on the left hand side to get a term of the form $1 + (n/q^{\frac{n}{6}})$. In the worst case $q = 2$, but $1 + (n/2^{\frac{n}{6}})$ is bounded because it converges to 0. Hence the above bound holds.

- > …The function $\delta(f)$ is 1 when f is square-free, and 0 otherwise. This is an easy consequence of unique factorization in A and the definition of square-free …

  To see this, just notice that choosing a term from the product on the left-hand side in

  $$\prod_P (1+\frac{1}{|P|^s}) = \sum \frac{\delta(f)}{|f|^s}$$

  is the same as choosing a monic polynomial (by choosing its prime factors) which is square free. So, by expanding the product on the left-hand side we can write it as a summation and it corresponds exactly to the sum on the right-hand side when we introduce the delta function.

Page 16

- > $$\lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} h(n) = \alpha$$

  There is a typo. The summand should read $h(k)$.

Page 17

- > $$\sum_f \left(\sum_{\substack{h,g \\ hg=f}} \frac{1}{|f|^s} \right) = \sum_f \frac{d(f)}{|f|^s} = \cdots$$

  The inner sum is indeed $d(f)$. To see this note that if $hg = f$ then h and g are both divisors of f. The map $(h,g) \mapsto h$ is a bijection between the pairs (h,g) and the divisors of f. Its inverse sends a divisor of f, say h, to the pair (h,g) where $hg = f$. Also, notice that (g,h) maps to the other divisor, namely g. So, we sum over $d(f)$ terms all of which are 1.

Page 18

- > …the above equation can be rewritten as $\sum_{g|f} \mu(g)|f/g| = (\mu * \lambda)(f)$ …

  By $|f/g|$ we mean $|f|/|g|$, or equivalently if $f = gh$, then by $|f/g|$ we mean $|h|$.

Page 19

- > …and collecting terms, we deduce
  >
  > $$S(n) = \sum_{k+l=m} q^k q^{2l}.$$
  >
  > The result follows after applying a little algebra …

  To get the result just factor out q^{2n} in the summand (the summand will become q^{-k}), and then sum the resulting geometric series.

§3 The Reciprocity Law

Page 23

- > …If $a \in A$ and P does not divide a, then, by Proposition 1.10 …

  The hypothesis is satisfied because $x^n - 1$ divides $x^m - 1$ if and only if n divides m. So in particular, $q - 1$ divides $q^d - 1 = |P| - 1$, implying d divides $|P| - 1$.

- > …The left-hand side of this congruence is, in any case, an element of order dividing d in $(A/PA)^*$ …

  Really we mean a representative of a class instead of element. More importantly, this means the left-hand side represents a d-th root of unity in $(A/PA)^*$.

Page 24

- > …there is a unique $\alpha \in \mathbb{F}^*$ such that
  > $$a^{\frac{|P|-1}{d}} \equiv \alpha \pmod{P}$$

  Indeed, the congruence above is true for some unique α. Recall that Corollary 1 to Proposition 1.9 says $(A/PA)^*$ contains all the d-th roots of unity. Also, $\mathbb{F}^*$ contains all the d-th roots of unity as well because d divides $q-1$. Now the injective map $\mathbb{F}^* \to (A/PA)^*$ is a homomorphism so it must take d-th roots to d-th roots.

- > …if two constants are congruent modulo P then they are equal …

  They are equal because if a and b are such constants, then $a-b$ (a constant) is a multiple of P (a polynomial) if and only if $a-b=0$.

- > …the map from $(A/PA)^* \to \mathbb{F}^*$ given by $a \mapsto (a/P)_d$ is a homomorphism whose kernel is the d-th powers in $(A/PA)^*$ by part 3 …

  Assertion 1 shows this map is well defined and assertion 2 shows it is a homomorphism.

- > …Since $(A/PA)^*$ is a cyclic group of order $|P|-1$, the order of the kernel is $(|P|-1)/d$ …

  Let the generator of the group be x. Then $x^d, x^{2d}, \ldots, x^{(|P|-1)}$ are all the d-th powers, and there are $(|P|-1)/d$ of them.

Page 25

- > …Using the theory of finite fields we find
  > $$P(T) = (T-\alpha)(T-\alpha^q)\cdots(T-\alpha^{q^{\delta-1}}) \quad \text{and}$$
  > $$Q(T) = (T-\beta)(T-\beta^q)\cdots(T-\beta^{q^{\nu-1}})$$

Recall from the theory of finite fields that the Frobenius map generates the Galois group. It follows that the map $x \mapsto x^q$ is an automorphism of $\mathbb{F}'$ since $q = p^f$. Now automorphism permute the roots of irreducible polynomials so $\alpha, \alpha^q, \ldots, \alpha^{\delta-1}$ are all roots of P (and similarly for β and Q). Since there are δ of these roots and P is a polynomial of degree δ (respectively ν for Q) we have found all the roots. Also notice that since $\mathbb{F}'$ contains α (and β) it contains all their powers and so P (and Q) split over $\mathbb{F}'$.

- > …Note that if $f(T) \in A'$ we have $f(T) \equiv f(\alpha) \pmod{(T-\alpha)}$ …

  To see this just collect terms of $f(T) - f(\alpha)$, and then notice that

  $$T^n - \alpha^n = (T-\alpha)(T^{n-1} + \alpha T^{n-2} + \cdots + \alpha^{n-1})$$

  for any $n \geq 1$ (where for $n = 1$ we just have $T - \alpha = T - \alpha$).

- > …note that if $g(T) \in A$ then $g(T)^q = g(T^q)$ which follows readily from the fact that the coefficients of $g(T)$ are in $\mathbb{F}$ …

  To see this just apply the Frobenius map to $g(T)$ and recall that it fixes $\mathbb{F}$.

- > …By symmetry this congruence holds modulo $(T - \alpha^{q^i})$ for all i and it follows that if holds modulo P.

  The symmetry we mean here is that since α was an arbitrary root of $P(T)$, the same argument holds for any other root of $P(T)$ which are precisely α^{q^i} for $i = 1, 2, \ldots, \delta - 1$. The congruence holding modulo P follows by the Chinese Remainder Theorem. Indeed, the prime ideals generated by the irreducibles polynomials $(T - alpha^{q^i})$ for all i are mutually co-prime because prime ideals in A are maximal and distinct maximal ideals are co-prime, and we have a congruence for each $(T - alpha^{q^i})$.

Page 27

- > …it is an interesting question to determine the number of d-th powers modulo m. Recall that we are assuming $d \mid (q-1)$. Under this assumption, the answer is $\Phi(m)/d^{\lambda(m)}$ where $\lambda(m)$ is the number of distinct monic prime divisors of m. This follows from Proposition 1.10 and the Chinese Remainder Theorem …

  Indeed, if we decompose $m = \alpha P_1^{e_1} P_2^{e_2} \cdots P_t^{e_t}$ into a product of its distinct monic prime divisors, then Proposition 1.10 tells us that the number of d-th powers modulo each of the factors is precisely $\Phi(P_i^{e_i})/d$. By the Chinese Remainder Theorem, a function is a d-th powers modulo m if and only if its a d-th power modulo $P_i^{e_i}$ for all i so that the number of d-th powers modulo m is precisely the product of the $\Phi(P_i^{e_i})/d$s which is $\Phi(m)/d^{\lambda(m)}$ because Φ is multiplicative.

Page 28

- > …we have $(m/P)_d = (P/m)_d$ and this gives the result by Part 3 of Proposition 3.1 and the fact that $(P/m)_d$ only depends on the residue class of P modulo m …

  To see this assume m is a d-th power modulo P. This is true if and only if $x^d = m \pmod{P}$ by definition which is true if and only if $(m/P)_d = 1$ by Proposition 3.1. So, this holds exactly when $(P/m)_d = 1$ by the proof. Now assertion 1 of Proposition 3.4 says if some $x = P \pmod{m}$, then $(P/m)_d = (x/m)_d$. This is what we mean by $(P/m)_d$ depends only on the reside class of P modulo m. Since the a_i are a full set of representatives for the classes of $(A/mA)^*$ such that $(a/m)_d = 1$ our previous statement holds exactly when $a_i = P \pmod{m}$ for some i.

- > …if $\deg(P)$ is odd, $(m/P)_d = 1$ iff $P \equiv b_i \pmod{m}$ for some i …

  To see this use the identity

  $$(m/P)_d = (-1)^{\deg(P)}(P/m)_d$$

, then multiply by -1, notice that the b_i are a full class of representatives modulo m for polynomials with this property, and finally use assertion 1 of Proposition 3.4.

Page 29

- > . . . By Theorem 2.2, there are infinitely many irreducibles of degree relatively prime to d. In fact, there are irreducibles of every degree . . .

  Indeed, there are at least q^n/n monic irreducible polynomials of each degree and there are infinitely many positive integers relatively prime to d.

- > . . . It then follows from equation (4) that $\mu^{\frac{q-1}{d}\deg(P)} = 1$ and so, $\mu^{\frac{q-1}{d}} = 1$. This shows that μ is a d-th power, $\mu = \mu_0^d$, in F . . .

  There is a typo, we mean $\mathbb{F}^*$ instead of F. The first statement here is clear. For the second, suppose $\mu^{\frac{q-1}{d}} \neq 1$ and set $x = \mu^{\frac{q-1}{d}}$. Then $x \in \mathbb{F}^*$ is not the identity and $|x|$ divides $\deg(P)$. But $|x|$ also divides d as well since $\mu \in \mathbb{F}^*$. Hence $|x|$ is a common divisor of $\deg(P)$ and d a contradiction. Therefore $\left(\frac{\mu}{P}\right)_d = 1$ which means μ is a d-th power in $\mathbb{F}^*$.