Projects for Math 371

Prof. Silberstein's Math 371 Class, Spring 2013

CHAPTER 1

Unique Factorization I

by Josh Cooper

(1) Define a UFD (unique factorization domain).

An *integral domain* is a nontrivial commutative ring R such that $\forall a, b \in R, ab = 0 \Rightarrow a = 0$ or $b = 0$. In other words, there are no zero divisors. For these definitions, assume R is an integral domain.

A *unit* is an element $u \in R$ such that u has an inverse element $u^{-1} \in R$, i.e., $uu^{-1} = u^{-1}u = 1$ (for example, in $\mathbb{Z}$, the only units are ± 1).

A non-zero, non-unit element $i \in R$ is said to be *irreducible* if it cannot be written as the product of two non-unit elements.

A non-zero, non-unit element $p \in R$ is said to be *prime* if $\forall x, y \in R$, p divides xy implies p divides x or p divides y.

We say that R has *existence of factorizations* if given a non-zero, non-unit element $r \in R$ we can factor r into irreducible elements γ_i and a unit a s.t. $r = a\left(\prod_{i=1}^{n} \gamma_i\right)$ for some non-negative n.

We can now define a *unique factorization domain* (UFD) as an integral domain that has existence of factorizations and the factorization is unique (that is unique up to multiplication by units or rearranging the terms being multiplied).

(2) Show that any PID is a UFD.

Recall the following definitions: $I \subset R$ is called an *ideal* if the following two properties hold:
(1) $i \in I$, $c \in R \Rightarrow ca \in I$.
(2) I is a subgroup of $(R, +, 0)$.
The ideal *generated by* $i_1, i_2, \ldots, i_n$ is defined as the smallest ideal containing these elements. I is said to be *principal* if it can be expressed as generated by only one element.
An integral domain R is a *principal ideal domain* (PID) if every ideal $I \subset R$ is principal.

THEOREM 1. *If R is a PID then R is a UFD.*

PROOF. Let R be a PID.

LEMMA 2. *Let $\alpha_1 R \subseteq \alpha_2 R \subseteq \ldots$ be an increasing sequence of ideals in R, then $\exists\ n$ s.t. $\forall m \geq n, \alpha_m R = \alpha_n R$.*

PROOF. Define
$$I = \bigcup_m \alpha_m R.$$
Then I is an ideal. To verify this fix $x_a, x_b \in I$ and WLOG $x_a \in \alpha_a R$ and $x_b \in \alpha_b R$. Let $l = \max\{a, b\} \Rightarrow \alpha_l R \subset I$ (because $l \in \mathbb{N}$) and we have $x_a, x_b \in \alpha_l R \Rightarrow x_a + x_b \in \alpha_l R \Rightarrow x_a + x_b \in I$. By similar reasoning, we have additive inverses and 0 in I so I is a subgroup of R over addition. Further, fix $i \in I, r \in R$. Say WLOG $i \in I_c \Rightarrow ir = ri \in I_c \Rightarrow ri \in I$. It follows that I is an ideal because both properties are met.
Now, because R is a PID, by definition, $\exists\ \omega \in R$ s.t. $I = \omega R \Rightarrow \omega \in I \Rightarrow \exists\ n$ s.t. $\omega \in \alpha_n R \Rightarrow \omega R \subseteq \alpha_n R \subseteq I$ but $I = \omega R$ so $I = \alpha_n R$ and thus $\forall m \geq n$, we have $\alpha_m R \subseteq I = \alpha_n R$ and $\alpha_n R \subseteq \alpha_m R$ (by definition) so we have $\alpha_m R = \alpha_n R$ as required. □

LEMMA 3. *Let $r \in R$ be non-zero and a non-unit. r can be factorized into irreducible elements.*

PROOF. Assume for contradiction that r cannot be factorized into irreducible elements. This implies r is not irreducible because otherwise $r = r$ would be the desired factorization. Thus, reduce r as $r = r_1 r_2$ where $r_1, r_2 \neq r$ and r_1 and r_2 are non-units. Because r cannot be factorized into irreducible elements, r_1 or r_2 cannot be factorized into irreducible elements. Say WLOG it is r_1. Consider $I_r := rR$ and $I_{r_1} := r_1 R$. We have $I_r \subseteq I_{r_1}$ and because r_2 is not a unit, $I_{r_1} \neq I_r$. We can apply the same process to r_1 and continue inductively to produce an increasing sequence of ideals such that no term is equal to the previous one. This contradicts Lemma 1.2 so the result follows. □

LEMMA 4. *Let $r \in R$ be irreducible. Then, r is prime.*

PROOF. By definition, we need to show that if r divides ab then r divides a or r divides b. Say r divides ab and WLOG that r does not divide a. We must show that this implies that r divides b. Let I be the ideal generated both by r and a. Because R is a PID, I is principal. The element that generates it must be both a factor of r and a, but because r is irreducible and does not divide a, we must have that $I = (1) = R$. This implies that $\exists\ \alpha, \rho$ such that $\alpha a + \rho r = 1 \Rightarrow \alpha ab + \rho rb = 1b = b$. Trivially, r divides ρrb and because r divides ab, r must divide $\alpha ab \Rightarrow r$ divides $\alpha ab + \rho rb = b \Rightarrow r$ divides b as required. □

LEMMA 5. *Fix $k, l \in \mathbb{N}$. Let $\alpha_i, 1 \leq i \leq k$ and $\beta_j, 1 \leq j \leq l$ be irreducibles and such that $\alpha_1 \alpha_2 \dots \alpha_k = \beta_1 \beta_2 \dots \beta_l$. It follows that $k = l$ and $\forall \iota, \exists\ \kappa_\iota$ s.t. κ_ι is a unit and $\beta_\iota = \kappa_\iota \alpha_\iota$ (after reordering).*

PROOF. Say WLOG $k \leq l$.
Case 1: $k = 0$. This gives $1 = \beta_1 \beta_2 \dots \beta_l \Rightarrow l$ must be 0 because each β_j term is irreducible and thus are non-invertible by defintion.
Case 2: $k = 1$. This gives $\alpha_1 = \beta_1 \beta_2 \dots \beta_l$. Assume $l \neq 1$. Then α_1 has a proper

factorization, which is a contradiction because it is irreducible. Thus $l = 1$ and $\alpha_1 = \kappa\beta_1$ for some unit κ.
Case 3: $k \geq 2$. For induction, assume that the statement holds for every value $h \leq k$ (the base cases are covered in Cases 1 and 2). By Lemma 1.4, we know that α_1 is prime and therefore α_1 divides one of the β_j terms. Reorder the β_j terms so that α_1 divides β_1. However, by definition, α_1 is not a unit and β_1 is irreducible so we have $\beta_1 = \alpha_1\kappa_1$ where κ_1 is a unit. This gives us $\alpha_1\alpha_2 \dots \alpha_k = \beta_1\beta_2 \dots \beta_l = \alpha_1\kappa_1\beta_2 \dots \beta_l \Rightarrow \alpha_2 \dots \alpha_k = \kappa_1\beta_2 \dots \beta_l$. By our inducitve hypothesis, it follows $k = l$. Further, $\forall \iota, \exists\ \kappa_\iota$ s.t. κ_ι is a unit and $\beta_\iota = \kappa_\iota\alpha_\iota$. □

Fix $r \in R$. By Lemma 1.3, r can be factorized into irreducible elements. By Lemma 1.5 this factorization is unique up to reordering and multiplying by units (because after reordering, we can always replace each β_ι term with $\kappa_\iota\alpha_\iota$ where κ_ι is a unit).
By definition, it follows that R is a UFD as required. □

(3) Deduce that if k is a field, then $k[x]$ is a UFD.
Let k be a field.

Theorem 6. *$k[x]$ is a UFD.*

Proof.

Lemma 7. *$k[x]$ is a PID.*

Proof. Let I be a non-empty ideal of the ring $k[x]$. Let $f(x)$ be a polynomial in I of minimal degree. Let $g(x)$ be any polynomial in I. By the division algorithm, $g(x) = h(x)f(x) + a(x)$ and the degree of $a(x)$ is strictly less than the degree of $f(x)$. But because $f(x)$ is of minimal degree, we have that $a(x) = 0 \Rightarrow g(x) = h(x)f(x) \Rightarrow I$ is generated by $f(x)$ and thus I is principal (note if I were trivial then it would be generated by 0 and would be principal). This implies the result. □

It follows from Lemma 1.7 and Theorem 1.1 that $k[x]$ is a UFD. □

(4) Deduce that $\mathbb{Z}$ is a UFD.

Theorem 8. *$\mathbb{Z}$ is a UFD.*

Proof.

Lemma 9. *$\mathbb{Z}$ is a PID.*

Proof. Let $I \subset \mathbb{Z}$ be an ideal of the ring $\mathbb{Z}$. Say $I = \{0\}$. I is now generated by 0. Otherwise, let s be the smallest positive element of I. Let (s) be the ideal generated by s alone. Because $s \in I$, we must have that every element of (s) is also an element of I so $(s) \subset I$. Now, consider $t \in I$. if $t = 0$ then $t \in (s)$ trivially. Say $t \neq 0$. We want to show that $t \in (s)$. Note that if $t \in (s)$ then $-t \in (s)$ so say WLOG that $t > 0$. By division (consider the Euclidean

algorithm), we know that $t = qs + r$ with $q, s, r \in \mathbb{N}$ and $0 \leq r < s$. Note that $s, t \in I \Rightarrow t - sq = r \in I \Rightarrow r = 0$ because s is the smallest positive integer in I and $0 \leq r < s$. Thus, $t = sq \Rightarrow t \in (s) \Rightarrow I \subset (s) \Rightarrow I = (s)$. Thus, any ideal can be generated by a single element, which implies the result. □

It follows from Lemma 1.9 and Theorem 1.1 that $\mathbb{Z}$ is a UFD. □

Citation: defintions and guidance were derived from *Algebra Abstract and Concrete. Edition 2.5* by Frederick M. Goodman and *Algebra* by Michael Artin.

CHAPTER 2

Unique Factorization II

by Xin Xiong

For this section, assume that R is a GCD domain.

DEFINITION 10. *Let R be an integral domain. If $\forall a, b \in R, \exists \gcd(a,b)$ s.t. $d \mid a, d \mid b$ iff $d \mid \gcd(a,b)$. We then see that $\gcd(a,b)$ is unique upto associates.*

DEFINITION 11. *$a, b \in R$ are associates in iff $\exists u \in R^\times$ s.t. $au = b$*

PROPOSITION 12. *$\mathbb{Z}[\sqrt{-5}]$ is not a UFD*

PROOF. Note that $2 \cdot 3 = (1+\sqrt{-5}) \cdot (1-\sqrt{-5}) = 6$. It suffices to show that $2, 3$ are irreducible in $\mathbb{Z}[\sqrt{-5}]$ and $(1+\sqrt{-5}), (1-\sqrt{-5})$ are not associates of 2. Consider $\mathbb{C} \supset \mathbb{Z}[\sqrt{-5}]$. Let $a, b, c \in \mathbb{R}$ with $(a,b) \neq (0,0)$. Then

$$\frac{c}{a+bi} = \frac{c(a-bi)}{a^2+b^2}$$

and thus $a \mid n$ iff $\bar{a} \mid n$. Consider $\|\cdot\| : \mathbb{C} \to \mathbb{R}, z = a+bi \mapsto a^2+b^2$ where $i = \sqrt{-1}$. Note that $\forall n \in \mathbb{Z}[\sqrt{-5}], \|n\| \in \mathbb{Z}$. Thus, we have

$$a, b \notin \mathbb{Z}[\sqrt{-5}]^\times, ab = 2 \Rightarrow \|a\|\|b\| = 4 \Rightarrow \|a\| = \|b\| = 2$$

and

$$c, d \notin \mathbb{Z}[\sqrt{-5}]^\times, cd = 3 \Rightarrow \|c\|\|d\| = 9 \Rightarrow \|c\| = \|d\| = 3$$

Since $\|a+b\sqrt{-5}\| = a^2+5b^2$, we may see that there are no such elements. Since $\|1+\sqrt{-5}\| = \|1-\sqrt{-5}\| = 6$, they are not associates of 2. □

DEFINITION 13. *Let $f = a_0 + \ldots + a_n X^n \in R[X]$. Then $\operatorname{cont}(f) = gcd(a_0, \ldots, a_n)$ (unique up to associates).*

Note that for the following, all choices yield equivalent results.

DEFINITION 14. *f is a primitive polynomial iff $\operatorname{cont}(f) = 1$*

THEOREM 15 (Gauß's Lemma). *If f, g are primitive polynomials in $R[X]$, then fg is a primitive polynomial.*

PROOF. Let $f = a_0 + \ldots a_m X^m, g = b_0 + \ldots b_n X^n$ and denote $m \coloneqq \deg f, n \coloneqq \deg g$. Obviously, this is true given $m = 0$ or $n = 0$. Now assume it is true for $(m, n-1)$ and $(m-1, n)$. We see that $fg = a_0 b_0 + (a_0 b_1 + a_1 b_0)X + \ldots + a_m b_n X^{m+n}$. Assume that for some prime p, $p \mid \operatorname{cont}(fg)$. Since $p \mid a_m b_n$, we have $p \mid a_m$ or $p \mid b_n$. We then have

$p \mid \text{cont}((f - a_m X^m)g)$ in the first case and $p \mid \text{cont}(f(g - a_n X^n))$ for the second case, both of which are impossible due to the inductive hypothesis. □

DEFINITION 16. *Let F be the field of fractions over R and let $f \in F[X]$ and $c \in R$ s.t. $cf \in R[X]$. Then $\text{cont}_F(f) = \frac{\text{cont}(cf)}{c}$. (again unique upto associates).*

COROLLARY 17. *Let $f, g \in F[X]$. Then $\text{cont}_F(fg) = \text{cont}_F(f)\,\text{cont}_F(g)$.*

PROOF. Let $a, b \in F[X]$ s.t. $af, bg \in R[X]$ are primitive. Then $\text{cont}(fg) = \frac{\text{cont}(afbg)}{ab} = \frac{\text{cont}(af)}{a} \cdot \frac{\text{cont}(bg)}{b} = \text{cont}\, f\, \text{cont}\, g$. Note that $f \in R[X]$ iff $\text{cont}_F(f) \in R$. □

COROLLARY 18. *Let $f \in R[X]$. Then f reducible in $R[X]$ iff reducible in $F[X]$.*

PROOF. Reducible in $R[X]$ implies reducible in $F[X]$ is trivial. For the other direction, let $c = \text{cont}\, f$ and $g = \frac{f}{c}$. Assume $f = pq$ for some $p, q \in F[X]$. Then we have $g = \frac{p}{c} \cdot q$ and $1 = \text{cont}\left(\frac{p}{c}\right)\text{cont}(q)$ and therefore $\text{cont}\left(\frac{p}{c}\right) = x, \text{cont}(q) = \frac{1}{x}$ for some $x \in F[X]$. Setting $p' = \frac{p}{cx}, q' = xq$, we have $p', q' \in R[X]$ and $f = cp'q'$. □

PROPOSITION 19. *$F[X]$ is a UFD.*

PROOF. We will show that $F[X]$ is a PID. By §1, we then have $F[X]$ is UFD. Let I be an ideal and let $f \in F[X]$ be an non-zero element of least degree. If f is a constant, we are done since F is a field. Assume otherwise. Now let $g \in I$. We then have $g = af + r$ for some $a, r \in F[X]$ where $\deg(r) < \deg(f)$.Since f is minimal, we have $r = 0$. □

PROPOSITION 20. *Let R be a UFD. Then R is a GCD domain.*

PROOF. Let $a = u\alpha_1 \dots \alpha_m, b = v\beta_2 \dots \beta_n \in R$ where $u, v \in R^\times$ and α_i, β_i irreducible and (α_i, β_i) are associates for $1 \leq i \leq t$ where $t \leq m, n$. We then have $\gcd(a, b) = \alpha_1 \dots \alpha_t$. □

THEOREM 21. *Let R be a UFD. Then $R[X]$ is a UFD.*

PROOF. Let $f \in R[X]$. We then have a unique factorization $f = cf_1 \dots f_n$ in $F[X]$ where $c = \text{cont}(f)$ and $\text{cont}(f_i) = 1$. By Gauß's lemma, $cf_1 \dots f_n$ is a unique factorization in $R[X]$. □

CHAPTER 3

Gauß' Lemma

by Zachary Goldsmith

1. Statement of Gauß' Lemma

Let $h \in \mathbb{Z}[x]$ be monic, and let $h = fg$ where $f, g \in \mathbb{Q}[x]$ and f monic. Then, $f, g \in \mathbb{Z}[x]$.

2. Proof

2.1. g is a monic polynomial. Let:

$$h = a_m x^m + a_{m-1} x^{m-1} + ... + a_1 x + a_0 \tag{1}$$

$$f = b_n x^n + b_{n-1} x^{n-1} + ... + b_1 x + b_0 \tag{2}$$

and

$$g = c_p x^p + c_{p-1} x^{p-1} + ... + c_1 x + c_0 \tag{3}$$

Since $h = fg$, $n + p = m$ and $a_m = b_n c_p$. Therefore, $c_p = \frac{a_m}{b_n}$. Since h and f are monic, $a_m = b_n = 1$. So, $c_p = 1$ and g is monic.

2.2. f and g actually have coefficients in $\mathbb{Z}$. Now, choose λ to be the smallest positive integer such that λf has integer coefficients. Note that the greatest common divisor of the coefficients of λf is 1. Similarly, choose ε to be the smallest positive integer such that εg has integer coefficients. Again, the gcd of the coefficients of εg is 1. Therefore:

$$\lambda f, \varepsilon g \in \mathbb{Z}[x] \tag{4}$$

Claim: $\lambda = \varepsilon = 1$
Assume $\lambda\varepsilon > 1$. Pick q such that q is prime and $q|(\lambda\varepsilon)$. Now consider:

$$\lambda\varepsilon h = (\lambda f)(\varepsilon g) \tag{5}$$

Now reduce this statement modulo q,

$$0 \equiv (\lambda f)(\varepsilon g) \tag{6}$$

Since $\mathbb{Z}/q\mathbb{Z}$ is an integral domain, so is $\mathbb{Z}/q\mathbb{Z}[x]$. Then,

$$\lambda f \equiv 0 \text{ or } \varepsilon g \equiv 0 \tag{7}$$

Therefore,

$$q|b_i \ \forall\ 0 \leq i \leq n \text{ or } q|c_j \ \forall\ 0 \leq j \leq p \tag{8}$$

In other words, q divides all of the coefficients of f or divides all of the coefficients of g.
$\Rightarrow\Leftarrow$ This is a contradiction to the assumption that $\lambda\varepsilon > 1$.

Thus, the claim that $\lambda = \varepsilon = 1$ is true and

$$f, g \in \mathbb{Z}[x] \tag{9}$$

CHAPTER 4

Maximal Orders in Quadratic Number Fields

by Assaph Aharoni

(1) Define an algebraic integer, and if $R \subseteq S$ define the integral closure of R in S. Prove that the integral closure of R in S is a ring.

Def: Let K be a finite field extension of $\mathbb{Q}$. An *algebraic integer* is a number in K that is a root of a monic integer polynomial. That is, $\alpha \in K$ is an algebraic integer if there exists $f(x) \in \mathbb{Z}[x]$ such that $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, $n \geq 1$, and $f(\alpha) = 0$.

Def: Let R and S be rings with $R \subseteq S$. We say $s \in S$ is *integral over* R if it is a root of a monic polynomial over R. That is , if $n \geq 1$ and $r_i \in R$ such that $s^n + r_{n-1}s^{n-1} + \cdots + r_1 s + r_0 = 0$. In other words, if there exists $f(x) \in R[x]$ such that $f(x)$ monic and $f(s) = 0$. The set of elements of S that are integral over R is called the *integral closure* of R in S.

We begin by proving the following lemma:

Lemma (1): For R and S defined as above, $s \in S$ is integral over R if and only if $R[s]$ is finitely generated as an R-module.

Proof:

"$\Longrightarrow$": Given s is integral over R, we want to show there exist $b_1, \ldots, b_m \in R[s]$ such that for all $f(s) \in R[s]$ there exist $r_1, \ldots, r_m \in R$ with $f(s) = \sum_{i=1}^{m} r_i b_i$. We know that for some $n \geq 1$ and ${r'}_i \in R$:

$$s^n + {r'}_{n-1}s^{n-1} + \cdots + {r'}_1 s + {r'}_0 = 0 \implies s^n = -{r'}_{n-1}s^{n-1} - \cdots - {r'}_1 s - {r'}_0$$

Let $f(s) \in R[s]$ be given by $f(s) = \sum_{i=0}^{N} c_i s^i$ with $c_i \in R$ and $N > n$. We can reduce the degree of $f(s)$ by 1 by making a substitution for s^n in the following manner:

$$f(s) = c_N s^{N-n} s^n + \cdots + c_0 = c_N s^{N-n}(-{r'}_{n-1}s^{n-1} - \cdots - {r'}_0) + \cdots + c_0 =$$

$$= {c'}_{N-1}s^{N-1} + \cdots + {c'}_0$$

This process can be repeated until the degree of $f(s)$ is down to $N - 1$.

$$f(s) = {c''}_n(-{r'}_{n-1}s^{n-1} - \cdots - {r'}_0) + \cdots + {c''}_0 = r_{n-1}s^{n-1} + \cdots + r_0$$

Therefore, if we let $b_1 = 1, b_2 = s, \ldots, b_m = s^{n-1}$, then we have shown that any element of $R[s]$ can be generated by linear combinations in R of these b_i's, i.e. $f(s) = \sum_{i=1}^{m} r_i b_i$. Since the number of b_i's is finite, $R[S]$ is finitely generated as an R-module.

"$\Longleftarrow$": Given that $R[s]$ is finitely generated, we want to show that s is integral over R. Let $\{b_1, b_2, \ldots, b_m\}$ be a generating set for $R[s]$, where $b_i = f_i(s)$ for some $f_i \in \mathbb{Z}[x]$. Let n be an integer such that $n > \deg(b_i)$ for $i = 1, \ldots, m$. Since s^n is an element of $R[s]$, we know that we can write it using the generating set ($r_j \in R$):

$$s^n = \sum_{j=1}^{m} r_j b_j \implies s^n - \sum_{j=1}^{m} r_j f_j(s) = 0$$

Let us define the polynomial $g(x) = x^n - \sum_{j=1}^{m} r_j f_j(x)$. $f(x)$ is monic because we defined all of the degrees of the elements in the generating set to be less than n and the x^n coefficient is 1, and it evaluates to 0 for the input s. Therefore, we have found $g(x) \in R[x]$ such that $g(x)$ is monic and $g(s) = 0$. Therefore, s is integral over R.

Claim: The integral closure C of R in S is a ring.

Proof: We proceed by proving that C is a subring of S. We must show C is closed under addition and multiplication. That is, for $x, y \in C \implies x \pm y \in C$ and $xy \in C$. First, by Lemma (1) we know that both $R[x]$ and $R[y]$ are finitely generated as R-modules. Let $1, x, x^2, \ldots, x^{n-1}$ span $R[x]$ and $1, y, y^2, \ldots, y^{m-1}$ span $R[y]$. It must be that $R[x, y]$ is also finitely generated by the elements $x^i y^j$ for $i \leq n, j \leq m$. Now consider the ring $R[x \pm y]$ which consists of elements $\sum_{i=0}^{N} r_i (x \pm y)^i$. Clearly, all of the elements of $R[x \pm y]$ are contained in $R[x, y]$, hence $R[x \pm y]$ is a submodule of $R[x, y]$ and is also finitely generated. Since $R[x \pm y]$ finitely generated, we have by Lemma (2) that $x \pm y$ is integral over R, i.e. $x \pm y \in C$. We make a similar argument that $R[xy]$ is a submodule of $R[x, y]$ and hence is also finitely generated, implying that xy is integral over R, i.e. $xy \in C$.

(2) Let K be a finite extension of $\mathbb{Q}$. Prove that the set $\mathcal{O}_K$ of algebraic integers in K is a subring of K and that the map $\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Q} \to K$ is an isomorphism.

Claim: The set $\mathcal{O}_K$ is a subring of K.

Proof: $\mathcal{O}_K$ is the set of elements α such that there exists a monic $f(x) \in \mathbb{Z}[x]$ for which $f(\alpha) = 0$. The integral closure of $\mathbb{Z}$ in K is the set of elements $b \in K$ such that b is integral over $\mathbb{Z}$, i.e. there exists a monic polynomial $f(x) \in \mathbb{Z}$ for which $f(b) = 0$. Clearly, the set of algebraic integers and the integral closure of $\mathbb{Z}$ in K are equivalent. By the proof of question 1 above, the integral closure of $\mathbb{Z}$

in K is a ring, which implies that $\mathcal{O}_K$ is a ring. Since $\mathcal{O}_K \subseteq K$, it is a subring of K.

Before discussing our second claim, we first prove the following lemma:

Lemma (2): For all $\beta \in K$, there exists an $m \in \mathbb{Z}$ such that $m\beta \in \mathcal{O}_K$.

Proof: Consider the polynomial $f(x) \in \mathbb{Q}[x]$ for which β is a root. Note that $f(x)$ must exist, otherwise $1, \beta, \beta^2, \dots$ would be linearly independent and K would be infinitely dimensional. Let $f(x) = \sum_{i=0}^{n} q_i \beta^i$, where $n \geq 1$ and $q_i \in \mathbb{Q}$. Let l be the lowest common multiple of all the r_i's.

$$f(\beta) = 0 \implies q_n\beta^n + q_{n-1}\beta^{n-1} + q_{n-2}\beta^{n-2} + \cdots + q_1\beta + q_0 = 0$$
$$lq_n\beta^n + lq_{n-1}\beta^{n-1} + lq_{n-2}\beta^{n-2} + \cdots + lq_1\beta + lq_0 = 0$$
$$p_n\beta^n + p_{n-1}\beta^{n-1} + p_{n-2}\beta^{n-2} + \cdots + p_1\beta + p_0 = 0$$

By multiplying both sides by l, we turn the coefficients into integers, i.e. $p_i \in \mathbb{Z}$. Now, we multiply both sides again by ${p_n}^{n-1}$:

$$(p_n\beta)^n + p_{n-1}(p_n\beta)^{n-1} + p_{n-2}p_n(p_n\beta)^{n-2} + \cdots + p_1{p_n}^{n-2}(p_n\beta) + p_0{p_n}^{n-1} = 0$$
$$(p_n\beta)^n + c_{n-1}(p_n\beta)^{n-1} + c_{n-2}(p_n\beta)^{n-2} + \cdots + c_1(p_n\beta) + c_0 = 0$$

Let $g(x) \in \mathbb{Z}[x]$ be such that $g(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0$. The p_i's multiplied all yield integers, hence $c_i \in \mathbb{Z}$. Therefore, we have found a monic polynomial $g(x) \in \mathbb{Z}[x]$ such that $g(p_n\beta) = 0$, i.e. $p_n\beta$ is an algebraic integer. If we let $m = p_n$, we have shown that there exists $m \in \mathbb{Z}$ such that $m\beta \in \mathcal{O}_K$.

Claim: The map $\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Q} \to K$ is an isomorphism.

Proof: Let $\varphi : \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Q} \to K, \alpha \otimes_{\mathbb{Z}} q \mapsto \alpha q$. To prove that φ is an isomorphism, we will argue that it is surjective and that the dimension of the domain is equal to the dimension of the codomain.

To prove φ is surjective, we have to show that any element $\beta \in K$ can be written as a product of $\alpha \in \mathcal{O}_K$ and $q \in \mathbb{Q}$. By Lemma (2), β can be written as $\alpha = m\beta$ for $m \in \mathbb{Z}, \alpha \in \mathcal{O}_K$. Since K is a field, we can write $\beta = \alpha\frac{1}{m}$, where $\frac{1}{m} \in \mathbb{Q}$. Therefore, we have shown that φ is a surjection.

Let $\dim_{\mathbb{Q}} K$ be n. If we can show that the dimension of $\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Q} \leq n$, we argue that φ is an isomorphism. In question 3, we prove that $\mathcal{O}_K$ is finitely generated as a $\mathbb{Z}$-module and that its rank is equal to $\dim_{\mathbb{Q}} K = n$. The tensor product map will have dimension equal to the product of $\mathcal{O}_K$'s rank and $\mathbb{Q}$'s dimension over itself, i.e. $\dim_{\mathbb{Q}}(\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Q}) = \text{rank}(\mathcal{O}_K)\dim_{\mathbb{Q}}(\mathbb{Q}) = n \cdot 1 = n$.

Now, since the tensor product is just a linear map, it preserves injectivity in each dimension. Therefore, since φ is surjective and the dimensions of its domain and codomain are equal, it must be the case that it is a bijection, i.e. φ is an isomorphism.

Note: Alternatively, one could prove the finite dimensionality by computing the

rank of the tensor product of $R[x]$ with $R[y]$ and noticing that it is finite.

(3) Prove that $\mathcal{O}_K$ is finitely generated as a $\mathbb{Z}$-module.

Def: Let $\alpha \in K$. We define the linear map $T_\alpha : K \to K, x \mapsto \alpha x$. We define the *trace* as the sum of the elements on the diagonal of the matrix representation of T_α. That is, $\mathrm{Tr}_{\mathbb{Q}}(T_\alpha) := \mathrm{Tr}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Q}$. Note that the trace is independent of the representation and is well-defined.

Claim: $\mathcal{O}_K$ is finitely generated as a $\mathbb{Z}$-module.

Proof: Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be a basis for K over $\mathbb{Q}$. Using Lemma (2) from above, we know that we can multiply the α_i's by an integer and get a new basis $\beta_1, \beta_2, \ldots, \beta_n$ such that each $\beta_i \in \mathcal{O}_K$. Consider the following map φ:

$$\varphi : K \to \mathbb{Q}^n, x \mapsto \big(\mathrm{Tr}_{K/\mathbb{Q}}(x\beta_1), \ldots, \mathrm{Tr}_{K/\mathbb{Q}}(x\beta_n)\big)$$

We claim that φ is injective. Suppose it is not, i.e. $\ker(\varphi) \neq \{0\}$. Let nonzero $y \in K$ be such that $\varphi(y) = 0$, i.e. $\mathrm{Tr}_{K/\mathbb{Q}}(y\beta_i) = 0$ for $i = 1, \ldots, n$. Notice the following:

$$n = \mathrm{Tr}_{K/\mathbb{Q}}(1) = \mathrm{Tr}_{K/\mathbb{Q}}(yy^{-1})$$

The first equality holds because the map $T_1 : K \to K, x \mapsto x$ has trace n since its matrix representation is simply the identity $n \times n$ matrix. The second equality holds because K is a field, so it has multiplicative inverses. Now, using our basis for K, we write $y^{-1} = \sum_{i=1}^{n} r_i\beta_i$ where the $r_i \in Q$.

$$\mathrm{Tr}_{K/\mathbb{Q}}(yy^{-1}) = \mathrm{Tr}_{K/\mathbb{Q}}\left(y\sum_{i=1}^{n} r_i\beta_i\right) = \mathrm{Tr}_{K/\mathbb{Q}}\left(\sum_{i=1}^{n} yr_i\beta_i\right) = \sum_{i=1}^{n} r_i\mathrm{Tr}_{K/\mathbb{Q}}(y\beta_i) = 0$$

We can move the trace inside the summation and factor out the r_i because the trace is a linear map. The final step comes from our assumption that $\varphi(y) = 0$. We have a clear contradiction: $n = 0$, even though we assumed that K is a finite field extension of $\mathbb{Q}$. Therefore, it must be the case that φ is indeed injective.

Now we look at the behavior of φ under $\mathcal{O}_K$, a subset of the domain. In φ under $\mathcal{O}_K$, α is mapped to a tuple of $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha\beta_i)$. Each $\alpha\beta_i \in \mathcal{O}_K$ because it is a product of two algebraic integers, and $\mathcal{O}_K$ is a ring according to question 2. We use without proof the fact that if $\alpha \in \mathcal{O}_K$, then $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$. Hence, each $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha\beta_i) \in \mathbb{Z}$. Therefore, the image of φ under $\mathcal{O}_K$ is $\mathbb{Z}^n \subseteq \mathbb{Q}^n$. By our argument above, φ is injective, implying that $\mathcal{O}_K$ is mapped injectively into $\mathbb{Z}^n$. We can view $\mathbb{Z}^n$ as a finitely generated abelian group and $\mathcal{O}_K$ as a subset of it, so $\mathcal{O}_K$ must be finitely generated as a $\mathbb{Z}$-module. In addition, since it is an n-tuple that depends on the basis of K and $\beta_1, \beta_2, \ldots, \beta_n$ are linearly independent, $\mathcal{O}_K$ has rank at least n. Since $\mathcal{O}_K$ injects into $\mathbb{Z}^n$, it has rank at most n. By the two previous statements, $\mathcal{O}_K$ must have rank exactly n.

CHAPTER 5

The Algebraic Integers in a Quadratic Number Field

by Benjamin Wang

Let $K = \mathbb{Q}(\sqrt{d})$. We define

$$\mathcal{O}_d = \{\alpha \in K \mid \alpha \text{ an algebraic integer}\}. \tag{10}$$

There is (a non-unique!) $\alpha \in K$ such that $\mathcal{O}_d = \mathbb{Z}[\alpha]$. Prove that we may take $\alpha = \frac{1+\sqrt{d}}{2}$ if $d \equiv 1 \pmod 4$ and $\sqrt{d}$ otherwise.

Proof: In this proof, we want to show that $\exists\, \alpha \in K = \mathbb{Q}(\sqrt{d})$ such that $\mathcal{O}_d = \mathbb{Z}[\alpha]$; that is, $\mathcal{O}_d = \{a + b\alpha \mid a, b \in \mathbb{Z}\}$.

To break down this proof, I will show two things:

(1) I will show that the fraction field $\mathbb{Q}(\sqrt{d})$ is isomorphic to $\mathbb{Q}[\sqrt{d}]$. This will give us information that allows us to make generalizations about any $\alpha \in \mathbb{Q}(\sqrt{d})$.
(2) Next, I will show, using Gauß' Lemma, that for arbitrary $\alpha \in \mathbb{Q}[\sqrt{d}]$ with the corresponding minimal polynomial f_α, $\alpha \in \mathcal{O}_d$ iff f_α has coefficients in $\mathbb{Z}$.

At this point, if I show these two things, then I only need to show the following equality: $\{\alpha' \in K | f_{\alpha'} \in \mathbb{Z}\} = \{a + b\alpha | a, b \in \mathbb{Z}[x]$ where $\alpha = \frac{1+\sqrt{d}}{2}$ if $d \equiv 1 \pmod 4$ and $\sqrt{d}$ otherwise$\}$

First, $\mathbb{Q}(\sqrt{d})$ is isomorphic to $\mathbb{Q}[\sqrt{d}]$.

$\mathbb{Q}$ is a field $\implies$ $\mathbb{Q}$ is a ring $\implies$ $\mathbb{Q}[\sqrt{d}]$ a ring. Since polynomial rings are always principal ideal domains, we can now check whether or not $\mathbb{Q}[\sqrt{d}]$ is a field. That is, we must show that $\forall\, \alpha \in \mathbb{Q}[\sqrt{d}]$ and $\alpha \neq 0, \exists\, \alpha^{-1}\, s.t.\, \alpha \cdot \alpha^{-1} = 1$.

Let $g \in \mathbb{Q}[x]$. Then, $g := q \cdot f_\alpha + r$ where r is the remainder polynomial. Substitute x for α, and we see that $g(\alpha) = r(\alpha)$, since $f_\alpha(\alpha) := 0$. Since f is irreducible, if $r \neq 0$, then $g.c.d.(f, r) = 1$ by definition of irreducible. Therefore, $\exists g'$, $h' \in \mathbb{Q}[x]\, s.t.\, g'\, f_\alpha + h'\, r = 1$. Evaluating at α yields $g_\alpha\, f_\alpha + h_\alpha\, r_\alpha = 1 \implies h_\alpha\, r_\alpha = 1 \implies r_\alpha = g_\alpha$ has an inverse in $\mathbb{Q}[\sqrt{d}]$. Therefore, $\mathbb{Q}[\sqrt{d}]$ is a field. Then, by definition of a fraction field, $\mathbb{Q}[\sqrt{d}] = \mathbb{Q}(\sqrt{d})$. To conclude this portion–since $\mathbb{Q}[\sqrt{d}]$ is isomorphic to $\mathbb{Q}[x]/(x^2 - D)$–we now know that by the division algorithm (and Homework 1) that $\alpha \in \mathbb{Q}[\sqrt{d}] = a + b\sqrt{d}$ for $a, b \in \mathbb{Z}$.

Now, we will prove the second step. Let $\alpha \in \mathbb{Q}(\sqrt{d})$ have minimal polynomial f_α.
Theorem: $\mathcal{O}_d := \{\alpha \in \mathbb{Q}(\sqrt{d}) | \alpha \text{ an algebraic integer}\} = \{\alpha \in \mathbb{Q}[\sqrt{d}] | f_\alpha \in \mathbb{Z}[x]\}$

"$\supseteq$" By definition of α being an algebraic integer.
"$\subseteq$" Gauß' Lemma, as so brilliantly presented by Zachary Goldsmith, states exactly this.

Now all we must show is that $(\mathcal{O}_d =)\{\alpha' \in K | f_{\alpha'} \in \mathbb{Z}[x]\} = \{a + b\alpha | a, b \in \mathbb{Z}$ where $\alpha = \frac{1+\sqrt{d}}{2}$ if $d \equiv 1 \pmod 4$ and $\sqrt{d}$ otherwise$\}(= \mathbb{Z}[\alpha])$.
"$\supseteq$" This direction is trivial, by definition. $(a, b, \alpha \in \mathcal{O}_d)$
"$\subseteq$" For arbitrary $\alpha' \in K$, let $\alpha' = a' + b'\sqrt{d}$ where $a', b' \in \mathbb{Q}$.

If $b' = 0$, then the minimal polynomial is $x - \alpha'$. In this simple case, the minimum polynomial has integer coefficients for any $a' \in \mathbb{Z}$. We can observe trivially that if $d \equiv 1 \pmod 4$, we can take $\alpha = \frac{1+\sqrt{d}}{2}$ and observe that α' has the form$a + b\alpha$ with $a, b \in \mathbb{Z}$ by letting $a = a'$ and $b = 0$. Similarly trivial, if $d \not\equiv 1 \pmod 4$, then we can take $\alpha = \sqrt{d}$, let $a = a'$ and $b = 0$.

Now, suppose $b' \neq 0$. Then, α' can be rewritten as $\frac{j+k\sqrt{d}}{l}$ where $j, k, l \in \mathbb{Z}$ and $g.c.d(j, k, l) = 1$. Given this α', the minimum polynomial can be expressed as $x^2 + px + q$, where $p = \frac{-2j}{l}, q = \frac{j^2-k^2d}{l^2}$. We get this by noticing that $(x - \frac{j+k\sqrt{d}}{l}) \cdot (x - \frac{j-k\sqrt{d}}{l})$–where $j, k, l \in \mathbb{Z}$ such that $p, q \in \mathbb{Q}$−−is a second degree polynomial (the lowest such polynomial) with α as a root and coefficients in $\mathbb{Q}$.

If $l = 1$, then any $j, k \in \mathbb{Z}$ works. Then $j + k\sqrt{d} \in a + b\alpha$ where $\alpha = \sqrt{d}, a = j \in \mathbb{Z}, b = k \in \mathbb{Z}$ or where $\alpha = \frac{1+\sqrt{d}}{2}$, $a = -j, b = 2k$.

If $l > 1$, then $l = 2$ in order that $p = \frac{-2j}{l} \in \mathbb{Z}$. From $q = \frac{j^2-k^2d}{l^2}$, q can only be integer when $g.c.d(j, l)^2 | k^2d \implies g.c.d(j^2, l^2) | k^2d$ (WHY? because $\frac{j}{l}$ and $\frac{k^2d}{l}$ must be integers.) Since $g.c.d(j, k, l) = 1$, $g.c.d(j, l) | d$. Since d is square-free,

$$g.c.d.(j, l) = 1. \tag{11}$$

Since $l = 2$ and q must be in $\mathbb{Z}$, this implies $4 | (j^2 - k^2d) \implies$

$$k^2d = j^2 \pmod 4. \tag{12}$$

By (2), $g.c.d(j, 2) = 1 \implies j$ must be odd. Similarly for k from (3). Therefore, $d \equiv 1 \pmod 4$. Conversely, if we assume $d \equiv 1 \pmod 4, j, k$ odd$, l = 2, p, q \in \mathbb{Z}$, then we work our way backwards to see that $\frac{j+k\sqrt{d}}{2}$ is an algebraic integer. Thus, $d \equiv 1 \pmod 4 \Leftrightarrow \frac{j+k\sqrt{d}}{2}$ is an algebraic integer.

Note then that we can take $\alpha = \frac{1+\sqrt{d}}{2}$, and for any $\frac{j+k\sqrt{d}}{2}$, we can express it in terms of $a + b\alpha$ where $a, b \in \mathbb{Z}$. Namely, we can let $b = k \in \mathbb{Z}$ and $a = \frac{j-k}{2} \in \mathbb{Z}$. Therefore, we have shown that $\exists\, \alpha \in K$ such that $\mathcal{O}_d \subseteq \mathbb{Z}[\alpha]$. Namely,

- $\alpha = \frac{1+\sqrt{d}}{2}$ if $d \equiv 1 \pmod 4$
- $\alpha = \sqrt{d}$ otherwise. (Notice that d cannot be $0 \pmod 4$ (or $4 \pmod 4$)). If it were, then we know that d would not be square free.). □

CHAPTER 6

Wedderburn's Theorem

by Archit Budhraja

1. Wedderburn's Theorem

Prove that any possibly noncommutative, finite ring R in which every nonzero element $r \in R$ has a multiplicative inverse, (that is, there is $r' \in R$ such that $rr' = r'r = 1$), is commutative.

2. Problem Statement

There is an equivalent restatement of Wedderburn's Theorem, which we will state in this section. But before that we must define certain terms required for this restatement.

Definition: A **division ring**, also called a **skew field** is a non-trivial ring in which every non-zero element r has a multiplicative inverse, i.e., an element x with $rx = xr = 1$.

So, from the above definition it is clear that the finite ring **R** in the statement of Wedderburn's Theorem is in fact a finite division ring. With this is mind, we can now restate the theorem as follows:

Prove that multiplication in a *finite* division ring is necessarily commutative.

3. Proof

Let **K** be a *finite* division ring.

Let **C**(x) be the *centralizer* in **K** of a nonzero element x.

Definition: The *centralizer* of a ring **R** is defined to be

$$C(R) = \{r \in R \,|\, rs = sr \text{ for all } s \in R\}. \tag{13}$$

Definition: The *centralizer* of an element $x \in \mathbf{R}$ is defined to be

$$C(x) = \{r \in R \,|\, rx = xr\}. \tag{14}$$

Now, we know that **C**(x) contains 0 and 1 and so it is trivial to establish that **C**(x) is a

subring of **K**, which contains the reciprocals of all its nonzero elements.

Let **C** be the *center* of **K**.

Definition: The *center* **C** of **K** consists of those elements of **K** which commute with *every* element of **K**.

So, from the above definition we know that

$$\mathbf{C} = \bigcap_{x \in \mathbf{R}} \mathbf{C}(x) \tag{15}$$

In particular, all elements of **C** commute, 0 and 1 are in **C** and so **C** is in fact a *field* of order q. Furthermore, we can also see that **K** and **C**(x) are vector spaces over **C**, with dimensions n and n(x) respectively.
Consider the multiplicative group formed by the q^n-1 nonzero elements of **K**. This group has center (**C** - {0}), which is of order q-1. We can then apply the conjugacy class formula to this group, but first we need to talk about what exactly the formula is.

3.1. Conjugacy class formula. Definition: Two elements x and y of a group **G** are said to be conjugates when there exists an inner automorphism from one element to the other, that is, when there is an element a of **G** such that $ax = ya$.

So defined, conjugacy is in fact an equivalence relation (it is reflexive, symmetric and transitive). The conjugacy class of an element x is the set of all elements of **G** which are conjugate to it. Every element is in one and only one of those classes since equivalence classes always form such a partition.

Furthermore, if x is in the center of **G**, denoted **Z(G)**, then the conjugacy class of x is simply x (a singleton set). More generally, it is the case that the number of elements that are conjugate to x is equal to the index in **G** of the centralizer **C**(x). That number is usually denoted [G : C].

Tallying the conjugacy classes with more than one element by assigning each a different index i, we obtain the conjugacy class formula:
|G| = |Z(G)| + $\sum_i$ [G : Ci]

The second term is an empty sum (equal to zero) when G is commutative.

Now, applying the conjugacy class formula to the group we discussed above, we get
q^n-1 = q-1 + $\sum_i$ (q^n-1)/(q^{n_i}-1)

Finally, to establish that multiplication is commutative, we need to prove that this above relation implies that $n = 1$, that is, the summation on the right-hand side must be empty. For this, we can utilize Zsigmondy's Theorem.

Zsigmondy's Theorem: If $1 \leq b < a$, and a and b are relatively prime, then a^n - b^n has at least one primitive prime factor with the following two possible exceptions:

(1) 2^6 - 1^6
(2) $n = 2$ and $a + b$ is a power of 2

Proof of Zsigmondy's Theorem: For a proof of this theorem, please refer to "Zsigmondy's Theorem" by Lola Thompson at `http://bit.ly/13EGlq1`.

Clearly the special cases of Zsigmondy's theorem (as stated above note) don't apply: Suppose $n = 2$. Since every term in the right-hand sum must be $(q^2\text{-}1)/(\text{q-}1) = (\text{q+}1)$, we see that it left-hand side is divisible by (q+1) but the right-hand side is not, which is a contradiction. Suppose $q = 2$ and $n = 6$. The class equation then reads

$$64 - 1 = 2 - 1 + \sum_i (2^6\text{-}1)/(2^{n_i}\text{-}1)$$

But, each term of the summation must equal $(2^6\text{-}1)/(2^2\text{-}1) = 21$ or $(2^6\text{-}1)/(2^3\text{-}1) = 9$ and so the class equation then becomes

$$62 = 21a + 9b$$

Now, we see that it right-hand side is divisible by 3 but the left-hand side is not, which is a contradiction.

Therefore, from Zsigmondy's theorem we can conclude that there is a prime p which divides $q^n\text{-}1$ but not $q^m\text{-}1$ for any positive value of m less than n (if any). Since such a p necessarily divides $q\text{-}1$ because it divides all other terms in the above equation, it must be the case that $n = 1$.

CHAPTER 7

The Derivative and Inseparable Polynomials

by Seth Koren

Let $f \in k[x]$, where k is a field. Define the **derivative** $D : k[x] \to k[x]$ to be the unique k-linear map which satisfies

(1) If $c \in k$ then $Dc = 0$.
(2) If $f, g \in k[x]$ then $D(fg) = fDg + gDf$.
(3) $Dx = 1$.

1. Roots of the Derivative

Let $(x - \alpha)|f$
To prove: $(x - \alpha)^2|f \Leftrightarrow (Df)(\alpha) = 0$
Proof:

1.1. "⇒". $(x - \alpha)^2|f$
$\Leftrightarrow f = (x - \alpha)^2 g$ with $g \in k[x]$
$\Rightarrow Df = gD(x - \alpha)^2 + (x - \alpha)^2 Dg$
$\Rightarrow Df = 2(x - \alpha)g + (x - \alpha)^2 Dg$
$\Rightarrow (Df)(\alpha) = 2(\alpha - \alpha)g + (\alpha - \alpha)^2 Dg = 0$

1.2. "⇐". $(Df)(\alpha) = 0$
$\Leftrightarrow (x - \alpha)|Df$
$\Leftrightarrow Df = (x - \alpha)g$ for some $g \in k[x]$
By proposition, $(x - \alpha)|f$, so $f = (x - \alpha)h$ for some $h \in k[x]$
So we know $Df = hD(x - \alpha) + (x - \alpha)Dh = h + (x - \alpha)Dh$
Thus $(x - \alpha)g = h + (x - \alpha)Dh$
$\Leftrightarrow g = \frac{h}{(x-\alpha)} + Dh$
Since $\frac{1}{(x-\alpha)} \notin k[x]$,$(x - \alpha)|h \Rightarrow h = (x - \alpha)l$ for some $l \in k[x]$
So $f = (x - \alpha)h = (x - \alpha)(x - \alpha)l$
Thus $(x - \alpha)^2|f$

□

2. Polynomials in $x^{char(k)}$

Let k be a field of characteristic p.
Let f be a polynomial with terms of degree only nonzero powers of p and zero; so

$$f = a_0 + \sum_{i=1}^{n} a_i x^{p^i}.$$

To prove: If an element $\alpha \in k'$, an extension of k, satisfies $f(\alpha) = 0$, then $(x-\alpha)^2 | f$

Proof:
$Df = D(a_0) + \sum_{i=1}^{n} a_i D(x^{p^i})$
$Df = \sum_{i=1}^{n} a_i p^i x^{p^i - 1}$
Since $p = 0$, $Df = 0$ identically
So for any root α of f in k', $(Df)(\alpha) = 0$
From 1, since $(x-\alpha)|f$ and $(Df)(\alpha) = 0$, $(x-\alpha)^2|f$
Since α was any root of f, any root of f is a multiple root.

□

3. Additivity of Polynomials in Finite Fields

To prove: If f is a polynomial with terms of degree only powers of p; so

$$f = \sum_{i=0}^{n} a_i x^{p^i}.$$

then f is additive, that is

$$f(x+y) = f(x) + f(y).$$

Proof:
$(x+p)^p = \sum_{i=0}^{p} \binom{p}{i} x^{p-i} y^i$ where $\binom{p}{i} = \frac{p!}{i!(p-i)!}$ by binomial theorem
For $i = 0$ or $i = p$, $\binom{p}{i} = 1$
If p is prime, then since $0 < i < p$, neither $i!$ nor $(p-i)!$ divide p.
But $\binom{p}{i}$ is always an integer.
So $p|\binom{p}{i}$ when p prime and $0 < i < p$
Thus, in a field of characteristic p, $(x+y)^p = x^p + y^p$
So $f(x+y) = \sum_{i=0}^{n} a_i (x+y)^{p^i} = \sum_{i=0}^{n} a_i (x^{p^i} + y^{p^i}) = f(x) + f(y)$ □

4. Testing Polynomial Irreducibility in Finite Fields

Let $f \in \mathbb{F}_q[x]$, $\deg(f) = n$, with $p_1, ..., p_k$ the distinct prime divisors of n.
To prove: f is irreducible $\Leftrightarrow$ ① $\gcd(f, x^{q^{\frac{n}{p_i}}} - x) = 1$ $\forall p_i$, and ② $f|(x^{q^n} - x)$
Proof:

4.1. "⇒". By assumption, f is irreducible.
For every root α of $f(x) = 0$, α is in $\mathbb{F}_{q^n} \simeq \mathbb{F}_q/f(x)$, which is n-dimensional over $\mathbb{F}_q$.
$\mathbb{F}_{q^n \setminus \{0\}}$ is a multiplication group of order $q^n - 1$, so by Lagrange's theorem the order of every element divides $q^n - 1$.
So $x^{q^n-1} = 1 \Rightarrow x^{q^n} - x = 0 \; \forall x \in \mathbb{F}_{q^n}$
Therefore $\alpha^{q^n} - \alpha = 0$, that is, α is a root of $x^{q^n} - x = 0$, so $(x - \alpha)|(x^{q^n} - x)$
Additionally, f has no multiple roots. We already have f irreducible, so $\gcd(f, g) \neq 1 \Rightarrow f|g \Rightarrow \deg(g) \geq \deg(f)$ or $g = 0$. But $\deg(Df) < \deg(f)$, so $\gcd(f, Df) = 1$ unless $Df = 0$.
However, if $Df = 0$, f is of the form seen in 2, above: $f = a_0 + \sum_{i=1}^{n} a_i x^{p^i}$. Since $x^p = x$ in $\mathrm{char}(p)$, $f = a_0 + \sum_{i=1}^{n} a_i x$, and then $x = \frac{-a_0}{\sum_{i=1}^{n} a_i}$ is a root of f in $\mathbb{F}_p$, which contradicts f irreducible in $\mathbb{F}_p$. Therefore, f has no multiple roots.
Thus, since $(x - \alpha)|(x^{q^n} - x)$ for every root α of $f(x)$, we have ② $f|(x^{q^n} - x)$
Now, since f is irreducible of degree n, $\mathbb{F}_{q^n}$ is the splitting field of f, and it therefore has no roots in any field $\mathbb{F}_{q^m}$ with $m < n$. Since $\frac{n}{p_i}$ integral $< n$, $(x - \alpha) \nmid (x^{q^{\frac{n}{p_i}}} - x)$ for any root α, thus ① $\gcd(f, x^{q^{\frac{n}{p_i}}} - x) = 1 \; \forall p_i$

4.2. "⇐". By assumption, ① $\gcd(f, x^{q^{\frac{n}{p_i}}} - x) = 1 \; \forall p_i$, and ② $f|(x^{q^n} - x)$
Since $f|(x^{q^n} - x)$, $(x - \alpha)|(x^{q^n} - x)$ for any root α, so all roots of f are in $\mathbb{F}_{q^n}$
Assume f has an irreducible factor f_1, of degree $m < n$.
The roots of f_1 are in $\mathbb{F}_{q^m}$, so $\mathbb{F}_{q^n}$ is a vector space over $\mathbb{F}_{q^m}$, and thus $m|n$.
Therefore $m|\frac{n}{p_i}$ for some p_i, so all roots of f_1 are in $\mathbb{F}_{q^{\frac{n}{p_i}}}$. But then $f_1|(x^{q^{\frac{n}{p_i}}} - x)$, and since $f_1|f$, then $f_1|\gcd(f, x^{q^{\frac{n}{p_i}}} - x)$, which contradicts ②.
Thus f is irreducible.

□

CHAPTER 8

Additive Polynomials

by Brandt Wong

Let k be a field of characteristic p. Prove that if $f \in k[x]$ is not a polynomial with terms of degree only powers of p, then f is not additive. (Hint: reduce to $\mathbb{F}_p$).
Note that in the finite field case, there are a number of polynomials such that $P(x+y) = P(x)+P(y)$ holds for all of the elements of the field. For example, over $\mathbb{F}_5$, $P(x) = x^6 - x^2$ is additive because it vanishes over the field in question. But this polynomial is not additive over the algebraic closure of $\mathbb{F}_5$. In this write up, we will find the general form of an additive polynomial over k and all field extensions of k, and then proceed to describe the general form of all additive polynomials over just the prescribed field, k.

First, we define an additive polynomial.

Definition: An additive polynomial is a polynomial $P \in k[x]$, such that, for $x, y \in k$, over any extension of k,

$$P(x+y) = P(x) + P(y). \tag{16}$$

Key Observations: $Q(x,y) = P(x+y) - P(x) - P(y) = 0$ over k for an additive polynomial, $P(x)$.

Note the difference between $Q(x,y)$ as an expression evaluated at points in a field and as a polynomial function of variables.

First we want to find the general form of an additive polynomial over a field k. We want to show that an additive polynomial can be written as the sum of polynomials that vanish over k and polynomials that are additive over k and all field extensions of k.

Proof: First we examine the case where k is infinite. Suppose $Q(x,y)$ is a polynomial where x and y are variables. We seek to find the kernel of the following map and we want to show that it is trivial.

$$k[x,y] \to Funct(k \times k, k)$$

That is, we want to show that if $\sum a_{ij}x^i y^j$ is 0, then a_{ij} are all 0. But we can reduce this to a one variable case if we fix y. Then we can get $f_y(x) = \sum a_{ij}y^j = 0$. If k is an infinite field, then all a_{ij}=0 by a simple counting argument: $\sum a_{ij}y^j = 0$ can only have finitely many zeros and thus cannot be zero over every element in the field. Thus, we need $\sum a_{ij}y^j = 0$ to be identically 0. So the kernel of the map is indeed 0.

Now we examine the finite field case.

Let k be the finite field, $\mathbb{F}_q$ where $q = p^d$. If P vanishes over $\mathbb{F}_q$, we want to show that P must then be a multiple of $x^q - x$. First we note that there is a bijection between polynomials of degree less than q and functions from $\mathbb{F}_q$ to $\mathbb{F}_q$. Moreover, this is also a

p-linear map. We can see that the map is bijective because there are q^q elements in each set and the map is injective, and therefore the map is also surjective. Since this map is bijective, we know that the kernel is trivial.

We know that $x^q - x$ vanishes over $\mathbb{F}_q$. We can establish another bijective mapping between the quotient ring over $x^q - x$ and functions from $\mathbb{F}_q$ to $\mathbb{F}_q$. Note that all polynomials will have remainders of degree less than q. Therefore, all polynomials over $\mathbb{F}_q$ can be mapped to their remainders when divided by $x^q - x$, and these remainders are mapped to functions from $\mathbb{F}_q$ to $\mathbb{F}_q$. Thus, the only polynomials that vanish are the ones that are multiples of $x^q - x$.

For any additive polynomial, $P(x)$, we can write

$$P(x) = h(x)(x^q - x) + r(x) \tag{17}$$

where the first part is a multiple of $x^q - x$ and therefore vanishes over $\mathbb{F}_q$. We want to show that $r(x)$ is such that $r(x)$ is additive over k and its extensions. There are $(q^d)^d$ p-linear maps between $\mathbb{F}_q$ and $\mathbb{F}_q$. Below we confirm that the only polynomials over k and all of its extensions are polynomials with terms of degree powers of p. There are $(q^d)^d$ of these as well. We know that $r(x)$ is a p-linear map and we know that all p-linear maps correspond to additive polynomials. So $r(x)$ is additive as well over k and all its extensions.

Therefore, we can now say that the general form for any additive polynomial over any field k, is the sum of additive polynomials over k and all field extensions, (the polynomials of the form described), and polynomials that vanish over the field, k. We proceed to find the general form of all additive polynomials over all field extensions of k.

Show that all additive polynomials over k and any extension of k have terms of degree only powers of p.

Proof: Suppose $P(x) = x^j$ is an additive monomial. Then for $j = 1$, $P(x+y)-P(x)-P(y)$ is true trivially. Suppose $j > 1$. Then $P(x + y) - P(x) - P(y)$ has a term, $jx^{j-1}y$. This will be identically zero only if $j = 0$ in characteristic p, that is, $j = 0 \pmod p$. So j must be a multiple of p.

Then we can write $j = p^k m$ where m does not divide p. If $P(x) = x^{p^k m}$ is additive, then $(x^{p^k} + y^{p^k})^m - (x^{p^k})^m - (y^{p^k})^m = 0$. This can only happen if $m = 1$, or, by the preceding reasoning, if m itself is a power of p, which would still mean j is a power of p.

So any additive monomial must have degree a power of p. Moreover, any sum or multiple of an additive monomial is also additive. It remains to show that a sum of non additive monomials is also not additive, that is, the linear combinations of additive monomials are the only additive polynomials.

Let $P(x) = c_1P_1(x) + c_2P_2(x) + ...c_nP_n(x)$, where each $P_i(x) = x^{j_i}$ is a monomial and at least one $P_i(x)$ is not additive.

Then

$P(x + y) - P(x) - P(y) = (c_1P_1(x + y) + c_2P_2(x + y) + ...c_nP_n(x + y)) - (c_1P_1(x) + c_2P_2(x) + ...c_nP_n(x)) - (c_1P_1(y) + c_2P_2(y) + ...c_nP_n(y)) = c_1(P_1(x + y) - P_1(x) - P_1(y)) + c_2(P_2(x + y) - P_2(x) - P_2(y)) + ...c_n(P_n(x + y) - P_n(x) - P_n(y))$

For each $P_i(x) = x^{j_i}$ that is not additive (j_i is not a power of p), then there will be a term $j_i x^{j_i - 1} y$ in the sum, and since all $P_i(x)$ are distinct, then there are no like terms to cancel out this non-zero term. So $P(x + y) - P(x) - P(y)$ does not equal 0 if at least one of the monomials is non-additive, and the desired result is proven. So for a field k of characteristic p, these are the only additive polynomials over k and all extensions of k.

CHAPTER 9

Artin-Schreier Extensions

by Himesh Lad

Let k be a field of characteristic p. The polynomial $\wp =_{\text{def}} x^p - x$ defines an additive function on k.

(1) Prove that the kernel of $\wp : k \to k$ is $\mathbb{F}_p$.
Proof: The map $\wp$ acts by sending $x \mapsto x^p - x$. So we are looking for the values of x which make $x^p - x$ equal to zero, i.e. the roots of the polynomial. If we consider elements of $\mathbb{F}_p$, we know that these satisfy the equation $x^p - x = 0$ because we are in a characteristic p field. We also know that there are a total of p elements in $\mathbb{F}_p$ and since there are at most p roots of $x^p - x$, it follows $\mathbb{F}_p$ is the kernel of $\wp$.

(2) Prove that if a field L containing k contains a β such that $\wp(\beta) = \alpha$, then the polynomial $\wp(x) - \alpha$ splits completely.
Proof: To show that $\wp(x) - \alpha$ splits completely we can simply find all the roots of the polynomial. For notation, let $f(x) =_{\text{def}} \wp(x) - \alpha$. We are already given that β is a root. Let us consider some $\beta + n$ for $1 \leq n \leq p$. Because $\wp$ is additive we have that $\wp(\beta + n) = \wp(\beta) + \wp(n) = \alpha + \wp(n) = \alpha + n^p - n$. However, since we are still in characteristic p, $n^p - n = 0$, thus $\wp(\beta + n) = \alpha$ so all roots are of the form $\beta + n$ and there are p of these roots. Since the deg $f(x) = p$, $f(x)$ splits completely.

(3) Prove that the polynomial $\wp(x) - \alpha$ is separable.
Proof: We have the following theorem:

Thm: A polynomial is separable iff the polynomial itself and its derivative have no common divisors

So clearly the derivative of $\wp(x) - \alpha = px^p - 1$. But since we are in characteristic p, $px^p - 1 = -1$ because $px^p = 0$. -1 clearly has no common divisors with $\wp(x) - \alpha$, thus $\wp(x) - \alpha$ is separable.

(4) Prove that if $\wp(x) - \alpha$ is irreducible, the splitting field L of $\wp(x) - \alpha$ has degree p over k, and has automorphism group $\mathbb{Z}/p$
Proof: The degree of the field extension of L for $f(x)$ over k is defined as $\dim_k L$. Since L is a splitting field for $f(x)$, f splits into linear factors in L. So we can generate L using k and the roots of $f(x)$. Thus the roots form a basis for L over

k, and since there are p roots, the $\dim_k(L) = p$. We saw in part 2 that every root is dependent on one root which we defined as β. That is, every root is defined as $\beta + n$ for $1 \leq n \leq p$. Since automorphisms permute the roots of $f(x)$, we only have to consider permutations of β, of which there are a total of p permutations. This is because every root is defined in terms of $\beta+n$, so for the automorphism to preserve structure, we can only permute where β goes, giving us p permutaions. Thus the automorphism group is isomorphic to $\mathbb{Z}/p$.

(5) Prove that if L/k is a field extension of degree p and $\mathrm{Aut}(L/k) = \mathbb{Z}/p$ then there is $\alpha \in k$ and $\beta \in L$ such that $f_\alpha(\beta) = 0$ and $\beta \notin k$. Such an element will be called an **Artin-Schreier root** of α and will be denoted by $\wp^{-1}(\alpha)$. It plays the role of a p-th root in characteristic p. When is $k(\wp^{-1}(\alpha)) \simeq k(\wp^{-1}(\alpha'))$?
Proof: Because L/k is a field extension of degree p with $\mathrm{Aut}(L/k) = \mathbb{Z}/p$, we know that L/k is cyclic of degree.
We then use the additive form of Hilbert's Theorem 90 which states the following *Let k be a field and L/k a cyclic extension of degree n with group G. Let σ be a generator of G. Let $\beta \in L$. The trace $Tr_k^L(\beta) = 0$ iff $\exists$ an element $\alpha \in L$ such that $\beta = \alpha - \sigma\alpha$*

Because we are in characteristic p the $Tr_k^L(-1) = 0$. If we let σ be the generator of the Galois group, then by Hilbert's theorem 90 we know that $\exists \beta \in L/k$ such that $\sigma\beta - \beta = 1$. Which implies $\sigma\beta = \beta + 1$. And then it follows that $\sigma^i\beta = \beta + n$ for $n = 1, ..., p$, and β has p distinct conjugates, which means that $[k(\beta) : k] \geqq p$. This then implies that the splitting field $L = k(\beta)$.

We now show that $\beta^p - \beta$ is fixed under σ.

$$\sigma(\beta^p - \beta) = \sigma(\beta)^p - \sigma(\beta) = (\beta + 1)^p - (\beta + 1) = \beta^p - \beta. \tag{18}$$

Since $\beta^p - \beta$ is clearly fixed under σ, powers of σ, and under G, it lies in the fixed field k. Thus by setting $\alpha = \beta^p - \beta$, then we have found an $\alpha \in k$ and a $\beta \in L$ such that $f_\alpha(\beta) = 0$ and $\beta \notin k$.

**Adapted from Lang's Algebra*

$k(\wp^{-1}(\alpha)) \simeq k(\wp^{-1}(\alpha'))$ when $f_{\alpha'} = f_\alpha$ and both irreducible in $k[x]$
This is due to the following proposition 9.2.1 from Goodman's *Algebra*:

Let k be a field and let $f(x)$ be a monic irreducible element of $k[x]$. If L and L' are field extensions of k containing elements α and α' satisfying $f(\alpha) = 0$ and $f(\alpha') = 0$, then there is an isophorphism $\psi : k(\alpha) \to k(\alpha')$ such that $\psi(k) = k$ for all $x \epsilon k$ and $\psi(\alpha) = \alpha'$.

Proof of Theorem: $k(\alpha) \cong k[x]/(f(x)) \cong k(\alpha')$ by isomorphisms that leave that leave k pointwise fixed.

CHAPTER 10

Finite Subgroups of the Multiplicative Group

by Chenchong Zhou

(1) Prove that every finite subgroup of the multiplicative group $k^\times$ of a field k is cyclic.

(2) Let k be of characteristic p. Prove that

$$\mathrm{Hom}(\mathbb{Z}/(p^n), k^\times) = \{x \in k^\times \mid x^{p^n} = 1\} \tag{19}$$

is the trivial group.

(3) Consider the polynomial $f(x) = x^{p^k} - x$. Prove that $f(x)$ is separable over any field k (hint: handle characteristic p and not p separately).

Proof.
Say A is a finite subgroup of $k^\times$ is the same as saying A is a finite subgroup of the group of all roots of unity in K. For $a \in A$, a has a finite order. Also for $n \geq 1$, $x^n = 1$ has at most n roots in K.
Let a be an element of such a subgroup A with the maximal order N. Let b be any element of A, n is its order. If $n \not| N$, by prime factorization, there is a prime p and a power of it $q = p^r$ such that $q|n$ and $q \not| N$.
Now claim that $ord(ab^{n/q}) = lcm(N, q) > N$ which contradicts the definition of N. (Note that N, q are coprime. Given a finite abelian group, $d = ord(ab), m = ord(a), n = ord(b)$, we know $d|lcm(m,n) = \frac{mn}{gcd(m,n)}$ and $\frac{mn}{gcd(m,n)^2}|d$)
Since $n|N$, $a^{iN/n} \in A$ with $0 \leq i < n$ are the n distincet roots of $x^n = 1$, and b is generated by $a^{N/n}$. This shows $a^{N/n}$ is a generator of A.

When k is of characteristic p, $x^{p^n} - 1 = 0$ is $(x-1)^{p^n} = 1$, so identity is the only solution and $\{x \in k^\times \mid x^{p^n} = 1\}$ is trivial.
Let a be the generator of $\mathbb{Z}/(p^n)$ since the group is cyclic. Let $f \in \mathrm{Hom}(\mathbb{Z}/(p^n), k^\times)$, note that f corresponds to $f(a) = b \in k^\times$ because f is defined as $f(a^k) = b^k$. Note that by definition of homomorphism, we also need $f(a^{p^n}) = b^{p^n} = 1$, so we have a bijection now.

Need to show $f(x)$ and $f'(x) = p^k x^{p^k - 1} - 1$ are coprime.
When k is of characteristic p, $f'(x) = -1$, so they are coprime.
When k is not of characteristic p, $f(x) = \frac{1}{p^k} f'(x) + (\frac{1}{p^k} - 1)x$.

$f'(x) = \frac{p^k}{1/p^k - 1} x^{p^k - 2}(1/p^k - 1)x - 1$, since the remainder from Euclidean Algorithm is a contant -1, $f(x)$ and $f'(x)$ are coprime.

CHAPTER 11

The Classification of Finite Fields

by Jason Liberman

Proposition 1: For every finite field k there is a natural number n so that k has cardinality p^n where p is the characteristic of k.

Proof. We have that k has prime characteristic p.

Lemma 1.1: k must contain a subfield isomorphic to $F = \mathbb{F}_p$.

Proof. Let us consider the ring homomorphism

$$\phi : \mathbb{Z} \longrightarrow k \tag{20}$$

$$n \longmapsto n \cdot 1_k \tag{21}$$

Now, from the first isomorphism theorem, we know that $\mathbb{Z}/ker\phi \cong im(\phi)$. But $im(\phi)$ is a subring because the image of a ring homomorphism is a subring. But any subring of a field is an integral domain so $im(\phi)$ is an integral domain. Then, $\mathbb{Z}/ker\phi$ is an integral domain because this property is preserved under isomorphism. It follows that $ker\phi$ is a prime ideal, for if not, there would be zero divisors in $\mathbb{Z}/ker\phi$. This implies that $ker\phi = \mathbb{Z}/p\mathbb{Z}$. Therefore, we conclude that $im(\phi)$ is not only a subfield, but also that $im(\phi) \cong \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$

k is a finite field, so the dimension of k as an F-vector space is finite. Let $dim_F k = n$. Then the basis of k as an F-vector space has n elements, each of which has coefficients in F. Because elements of k can be written uniquely in terms of the basis elements over F, there are p^n elements of k.

□

Proposition 2: Prove that a finite field k of cardinality p^n is the splitting field of the polynomial $f(x) = x^{p^n} - x$ over $\mathbb{F}_p$.

Proof. We will show that a field has finite cardinality p^n if and only if it is the splitting field of $f(x) = x^{p^n} - x$ over $\mathbb{F}_p$.

($\Rightarrow$) We want to show that if k is a finite field of order p^n, $f(x)$ splits completely in k, and the roots of $f(x)$ generate k over $\mathbb{F}_p$. Let $m = p^n$. Consider the multiplicative group $k^\times$. This group has order $m-1$ because it contains all elements in k excluding 0. Therefore, the order of $\alpha \in k^\times$ divides $m-1$, so $\alpha^{m-1} = 1$.

Now, we have that

$$x^m - x = x(x^{m-1} - 1) \tag{22}$$

Because $\forall \alpha \in k^\times$, $\alpha^{m-1} - 1 = 0$, all elements of $k^\times$ are roots of x^m - x. But 0 is also a root. Therefore, every element of k is a root of x^m - x. But we also know from project 10, part 3, that $f(x)$ is separable over any field. Therefore, it has m distinct roots. Then the elements of k are precisely the distinct m roots of $f(x)$. Also, the roots generate k over $\mathbb{F}_p$ since they form a field which contains $\mathbb{F}_p$. Therefore, k is a splitting field of $f(x) = x^{p^n} - x$ over $\mathbb{F}_p$.

($\Leftarrow$)Now, let us show that the splitting field L of $f(x) = x^{p^n} - x$ over $\mathbb{F}_p$ is a finite field of order p^n. We know that there are p^n distinct roots of f in L. First, let us show that these p^n distinct roots form a subfield $K \subseteq L$.

Lemma 2.1: In $\mathbb{F}_p[x, y]$, $(x+y)^m = x^m + y^m$ where $m = p^n$.

Proof. Use induction on n. When $n = 1$,

$$(x+y)^p = x^p + \binom{p}{1}x^{p-1}y + \cdots + \binom{p}{p-1}xy^{p-1} + y^p \tag{23}$$

But then, all of the middle terms are divisible by p, so they are all equal to zero in $\mathbb{F}_p[x, y]$. Therefore, we have that $(x+y)^p = x^p + y^p$.

Now, we suppose the statement is true for some $n > 1$. Then,

$$(x+y)^{p^{n+1}} = (x+y)^{(p^n)p} = (x^{p^n} + y^{p^n})^p = x^{p^{n+1}} + y^{p^{n+1}} \tag{24}$$

So by induction, we have that in $\mathbb{F}_p[x, y]$, $(x+y)^m = x^m + y^m$ where $m = p^n$.

□

Now, let us show that the roots of $f(x) = x^{p^n} - x$ form a subfield $K \subseteq L$. Suppose α and β are two roots. We must show that $\alpha + \beta$, $-\alpha$, $\alpha\beta$, α^{-1}, and 1 are all roots. From the lemma above, we know that $(\alpha+\beta)^m = \alpha^m + \beta^m = \alpha + \beta$. So $(\alpha+\beta)^m - (\alpha+\beta) = 0$. Then $(\alpha\beta)^m - \alpha\beta = \alpha^m\beta^m - \alpha\beta = \alpha\beta - \alpha\beta = 0$. 1 is a root since $1^m - 1 = 0$. Also, $(\alpha^{-1})^m - \alpha^{-1} = \alpha^{-m} - \alpha^{-1} = \alpha^{-1} - \alpha^{-1} = 0$. In order to show that $-\alpha$ is a root, let us show that -1 is a root. If $p = 2$, $(-1)^m = 1$, and $(-1)^m + 1 = 0$ since then $char(L) = 2$. If $p \neq 2$, then $(-1)^m = -1$ so -1 is a root. Therefore, $-\alpha$ is a root since -1 and α are.

Next, let us show that $\gamma \in \mathbb{F}_p$ is a root of f. If $\gamma = (1 + 1 + \cdots + 1)$, then $\gamma^m - \gamma = (1 + 1 + \cdots + 1)^m - \gamma = (1^m + \cdots + 1^m) - \gamma = 0$.

We have shown that the roots of $f(x) = x^{p^n} - x$ over $\mathbb{F}_p$ form a subfield $K \subseteq L$. But then $x^{p^n} - x$ splits into linear factors in K, and clearly K is generated by the roots of f over $\mathbb{F}_p$, which K contains. But then by the minimality of the splitting field, K is the splitting field, and it has order $m = p^n$. Therefore, the splitting field of f is a finite field of order p^n.

□

Proposition 3: Any two finite fields of the same cardinality are isomorphic.

Suppose k and k' are two finite fields of order p^n. From Project 10, part 1, we know that every finite subgroup of the multiplicative group of a field is cyclic. Since $k^\times$ is finite, it is a finite subgroup of itself. Therefore, $k^\times$ is cyclic. Therefore, $k = F(\alpha)$ where α is the generator of $k^\times$.

We know that α is algebraic over F because it must be a root of $x^{p^n} - x$. Therefore, there is a unique minimal polynomial, $g(x) \in k(x)$ such that $g(x)$ divides all of the polynomials with root α. Then, we have that:

$$deg(g(x)) = dim_F(F(\alpha)) = n \tag{25}$$

$$F(\alpha) \cong F[x]/(g(x)) \tag{26}$$

Since α is a root of $x^{p^n} - x$, g must divide $x^{p^n} - x$.

Now, we also know that $x^{p^n} - x$ splits into linear factors in k'. So g has a root α' in k'. α' is algebraic over F, so $g(x)$ is the minimal polynomial for α' over F. Therefore, we have that

$$deg(g(x)) = dim_F(F(\alpha')) = n \tag{27}$$

$$F(\alpha') \cong F[x]/(g(x)) \cong F(\alpha) \tag{28}$$

Now, all that is left to show is that $F(\alpha') = k'$. Both $F(\alpha')$ and k' are vector spaces over $\mathbb{F}_p$, and $dim_F(k') = n = dim_F(F(\alpha))$. Therefore, we conclude that:

$$k \cong F(\alpha) \cong F(\alpha') \cong k' \tag{29}$$

□

CHAPTER 12

The Euler Totient Function

by Andrei Nagornyi

Let $\varphi(n)$ be the Euler totient function:

$$\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^{\times}. \tag{30}$$

1. Closed form of $\varphi(n)$

PROOF. Recall from class that given a universal set U and subsets $A_1, A_2, \ldots, A_m$ of U, $|\overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_m}| = |U| - \sum_i |A_i| + \sum_{i<j} |A_i \cap A_j| - \sum_{i<j<k} |A_i \cap A_j \cap A_k| + \ldots + (-1)^m |A_1 \cap \ldots \cap A_m|$. Now, let $n \in \mathbb{Z}^+$ and $U = \{x \mid 0 < x \leq n\}$. Let $p_1^{r_1} p_2^{r_2} \ldots p_h^{r_h}$ denote the prime factorization of n, and define the collection of subsets of U, $A_i = \{x \mid p_i | x,\ 0 < x \leq n\}$ for $1 \leq i \leq k$. It is clear that $\varphi(n) = |\overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_n}| = |U| - \sum_i |A_i| + \sum_{i<j} |A_i \cap A_j| - \sum_{i<j<k} |A_i \cap A_j \cap A_k| + \ldots + (-1)^n |A_1 \cap \ldots \cap A_h|$. We now make the observation that $|A_{j_1} \cap \ldots \cap A_{j_s}| = n \cdot \frac{1}{p_{j_1} \ldots p_{j_s}}$. After making this substitution, we have $\varphi(n) = n - \sum_i \frac{n}{p_i} + \sum_{i<j} \frac{n}{p_i p_j} - \sum_{i<j<k} \frac{n}{p_i p_j p_k} + \ldots + (-1)^h (\frac{n}{p_1 \ldots p_h}) = n(1 - \frac{1}{p_1}) \ldots (1 - \frac{1}{p_h}) = n \prod_{p_i | n} (1 - \frac{1}{p_i})$. □

2. The totient function is multiplicative

Prove that if $(m, n) = 1$ then $\varphi(mn) = \varphi(m)\varphi(n)$.

PROOF. If $(m, n) = 1$, then by the Chinese Remainder Theorem, we have $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Consequently, we also have $(\mathbb{Z}/mn\mathbb{Z})^{\times} \cong (\mathbb{Z}/m\mathbb{Z})^{\times} \times (\mathbb{Z}/n\mathbb{Z})^{\times}$. Hence, $\varphi(mn) = \varphi(m)\varphi(n)$. □

3. If a field k contains a primitive m-th root of unity, then k contains all m-th roots of unity.

PROOF. Let g be a subgroup of the multiplicative group $k^{\times}$ consisting of all m-th roots of unity. Note that g must be finite since the polynomial $x^m - 1$ will have at most m distinct roots. We also know that g must be cyclic, based on the first result of project 10. Then, since k contains a primitive m-th root of unity z, we have $z^m = 1$. It is clear that z is a generator of g, and hence of all the m-th roots of unity of k. □

CHAPTER 13

The Totient Function II

(1) For each $m \in \mathbb{N}$, define $\Xi_m = x^m - 1$. If k is a field, we denote by ζ_m a primitive m-th root of unity and thus $k(\zeta_m)$ the splitting field of Ξ_m. Prove that there is a natural injection $\mathrm{Aut}(k(\zeta_m)/k) \to (\mathbb{Z}/m)^\times$ so $\dim_k k(\zeta_m) \leq \varphi(m)$.
(2) Prove that $\dim_{\mathbb{Q}} \mathbb{Q}(\zeta_m) = \varphi(m)$. (Hint: induction on the number of divisors of m).

From here on out, we define $\Gamma_m =_{\mathrm{def}} \mathrm{Aut}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) = (\mathbb{Z}/m)^\times$.

CHAPTER 14

The Classification Theorem for Finitely-Generated $\mathbb{Z}$-modules: Part I

Let M be a finitely-generated abelian group. Prove that there exists a natural number n, primes $p_1, \ldots, p_n$, and for each p_i natural numbers $e_{j1}, \ldots, e_{j\ell_i}$ and $r_{j1}, \ldots, r_{j\ell_i}$ such that

$$M \simeq \mathbb{Z}^n \oplus \prod_{i=1}^{n} \prod_{j=1}^{\ell_i} (\mathbb{Z}/p^{e_{ji}})^{r_{ji}} \tag{31}$$

CHAPTER 15

The Classification Theorem for Finitely-Generated $\mathbb{Z}$-modules: Part II

by Rami Sherif

1. Given an abelian group M, show that the numbers n, p_i, ℓ_i, e_{ji} and r_{ji} can be determined independently of the decomposition from question 14.

To begin, we will assume the decomposition from part 14 and rewrite it as follows: For M a finitely generated abelian group,

$$M \simeq \mathbb{Z}^n \oplus \prod_{p,e} (\mathbb{Z}/p^e)^{r(p,e)} \tag{32}$$

We want to show that this decomposition is unique. I.e. we want to show that n and $r(p,e)$ are unique, as if these two are unique than the rest of the uniqueness follows.

1.1. Considerations. To start, let us consider the following tensor products:
(1) $\mathbb{Q} \otimes \mathbb{Z}$
Anything tensor $\mathbb{Z}$ is equal to itself, so, $\mathbb{Q} \otimes \mathbb{Z} = \mathbb{Q}$.
(2) Similarly, $\mathbb{Z} \otimes \mathbb{Z}/n = \mathbb{Z}/n$
(3) $\mathbb{Q} \otimes \mathbb{Z}/n$
This is generated by a⊗b, a $\in \mathbb{Q}$, b $\in \mathbb{Z}$. In $\mathbb{Q}$, division by n $\in \mathbb{Z}$ in allowed. Let a=n(a/n). a⊗b=n(a/n)⊗b. By bi-linearity of tensor products, n(a/n)⊗b=((a/n)⊗b)n=(a/n)⊗(bn)=0, since bn$\in \mathbb{Z}/n$.
Thus, $\mathbb{Q} \otimes \mathbb{Z}/n = 0$
(4) $\mathbb{Z}/p^e \otimes \mathbb{Z}/p^f$ where p is some prime and $e \neq f$
$\mathbb{Z}/p^e \otimes \mathbb{Z}/p^f = (\mathbb{Z}/p^e\mathbb{Z})/((p^f\mathbb{Z}/p^f\mathbb{Z}) = \mathbb{Z}/(p^e\mathbb{Z} + p^f\mathbb{Z})$
$(p^e\mathbb{Z} + p^f\mathbb{Z}) = (p^{\min(e,f)}\mathbb{Z}) \Rightarrow \mathbb{Z}/p^e \otimes \mathbb{Z}/p^f = \mathbb{Z}/(p^{\min(e,f)})$

1.2. Proof of Uniqueness. Now let us go back to the decomposition defined by equation (1). Consider,

$$M \otimes \mathbb{Q} \tag{33}$$

Using (1) and (2) from the tensor products we considered above, tensoring with $\mathbb{Q}$ will send all $\mathbb{Z}$ to $\mathbb{Q}$ and any other term $\in M$ to 0. Thus,

$$M \otimes \mathbb{Q} \simeq \mathbb{Q}^n \tag{34}$$

Or, in other words, $M \otimes \mathbb{Q}$ is isomorphic to the direct sum of $\mathbb{Q}$ with itself, n times. When we tensor M with $\mathbb{Q}$, we get a series of n terms and that n is specific to that decomposition of M. Any different decomposition of M will result in a different tensor product with $\mathbb{Q}$ with $m \neq n$ terms.

Thus, n is unique.

Now, we claim that all $r(p, e)$ in the above decomposition of M are unique. Consider,

$$M \otimes \mathbb{Z}/p \simeq (\mathbb{Z}/p)^x \tag{35}$$

This tensor product results in an abelian group where $x = n + \sum_{e=1}^{\infty} r(p, e)$= the number of terms in the tensor product. This can be explained as follows: in the tensor product, each $\mathbb{Z}/p$ will hit a series of $\mathbb{Z}$s from the $(\mathbb{Z})^n$ portion of the decomposition giving n terms. Then, each $\mathbb{Z}/p$ will hit everything else $\in \mathbb{M}$, and by tensor product number (4) considered at the beginning of this proof, all of the terms will go to $\mathbb{Z}/p$. The group $\mathbb{Z}/p$ has order p, while the group $(\mathbb{Z}/p)^2$ has order p^2. Therefore, the group $(\mathbb{Z}/p)^x$ has order p^x, where $x = n + \sum_{e=1}^{\infty} r(p, e)$.

Similarly, consider,

$$M \otimes \mathbb{Z}/(p^2) \simeq (\mathbb{Z}/p^2)^n \bigoplus (\mathbb{Z}/p)^c \bigoplus (\mathbb{Z}/p^2)^d \tag{36}$$

n was uniquely determined in the beginning of this proof. The first term is a result of $\mathbb{Z}/p^2$ hitting $\mathbb{Z}^n \in M$. The second term is a result of $\mathbb{Z}/p^2$ hitting any term $\mathbb{Z}/p \in M$ and following from tensor product (3) considered above. $c = r(p, 1)$ since it is all terms with $e = 1$. Finally, the last term is a result of $\mathbb{Z}/p^2$ hitting any term $\mathbb{Z}/(p^e) \in M$ for any $2 \leq e$, also according to tensor product (3) that we considered. So, $d = \sum_{e=2}^{\infty} r(p, e)$. Thus the total number of terms in (5) is $n + r(p, 1) + \sum_{e=2}^{\infty} r(p, e)$.

Following the same reasoning as before, $(\mathbb{Z}/p)$ has order p and $(\mathbb{Z}/p)^2$ has order p^2, so $(\mathbb{Z}/p^2)^n \bigoplus (\mathbb{Z}/p)^c \bigoplus (\mathbb{Z}/p^2)^d$ has order $p^{2n+c+2d} = p^{2n+r(p,1)+2\sum_{e=2}^{\infty} r(p,e)}$.

Suppose, now, that we wanted to isolate a specific $r(p, e)$ to show that any r can be shown to be unique for a given p. Let's try and show that $r(p, 1)$ is unique. Take the two group orders that were determined above.

$$Ord(M \otimes \mathbb{Z}/p) = p^{n+\sum_{e=1}^{\infty} r(p,e)} \tag{37}$$

$$Ord(M \otimes \mathbb{Z}/(p^2)) = p^{2n+r(p,1)+2\sum_{e=2}^{\infty} r(p,e)} \tag{38}$$

Now, let us take the $\log_p$ of both of the above equations:

$\log_p[\mathrm{Ord}(M \otimes \mathbb{Z}/p)]=\log_p[p^{\mathrm{n}+\sum_{\mathrm{e}=1}^{\infty} \mathrm{r(p,e)}}] \to \log_p[Ord(M \otimes \mathbb{Z}/p)] = n + \sum_{e=1}^{\infty} r(p,e)$

Similarly, for (7):

$$\log_p[Ord(M \otimes \mathbb{Z}/(p^2))] = \log_p[p^{2n+r(p,1)+2\sum_{e=2}^{\infty} r(p,e)}]$$

$$\to \log_p[Ord(M \otimes \mathbb{Z}/(p^2))] = 2n + r(p,1) + 2\sum_{e=2}^{\infty} r(p,e)$$

From this, we can easily isolate a specific r, say $r(p,1)$:

$$r(p,1) = \log_p(Ord(M \otimes \mathbb{Z}/(p^2))) - 2[\log_p(Ord(M \otimes \mathbb{Z}/p)] \tag{39}$$

Thus, we can see that r(p,1) can be isolated and written uniquely.

This can be continued for all e by taking $M \otimes \mathbb{Z}/(p^e)\ \forall\ e$ and getting a term $r(p, e-1)$ within the sum defining the number of terms within the tensor product. From here, it is obvious that we can continue to tensor M with $\mathbb{Z}/(p^x)\ \forall\ x$ until we get a system of equations that can be manipulated using simple arithmetic to isolate $r(p,e)$ for any given p.

Finally, it should be noted that if M were at all different from the decomposition defined at the beginning of this proof, all of the tensor products would result in different answers and thus give different values for r and n.

Since both n and r are found to be unique for any given p, it follows that all bounds are unique to the particular abelian group and can be independently determined.

□

2. Given M, M' two finitely-generated $\mathbb{Z}$-modules, prove that an injective map $i : M \to M'$ has image of finite-index if and only if $M \simeq \mathbb{Z}^n \oplus F$ and $M' \simeq \mathbb{Z}^n \oplus F'$ where F and F' are finite abelian groups.

We showed above that n is unique. Since n is unique, it is called the rank of the abelian group. M is a submodule of M'. If the image is of finite index, then the quotient group is finite. In other words, we want to show that the image is of finite index if and only if M and M' have the same rank.

$\Rightarrow$

Assume that the image of the map i is of finite-index. Consider the following direct sequence:

$$0 \to M \to M' \to M'/M \to 0 \tag{40}$$

Now let us tensor this entire sequence with $\mathbb{Q}$:

$$[0 \to M \to M' \to M'/M \to 0] \otimes \mathbb{Q} = 0 \otimes \mathbb{Q} \to M \otimes \mathbb{Q} \to M' \otimes \mathbb{Q} \to (M'/M) \otimes \mathbb{Q} \to 0 \tag{41}$$

$0 \otimes \mathbb{Q}$ remains 0 since $\mathbb{Q}$ is a flat $\mathbb{Z}$-module, i.e. $\mathbb{Q}$ preserves sequences. Additionally, $(M'/M) \otimes \mathbb{Q}$ goes to 0 since we are assuming that (M'/M) is a finite group.

Thus, we are left with:

$$0 \to M \otimes \mathbb{Q} \to M' \otimes \mathbb{Q} \to 0 \tag{42}$$

In direct sequences, the image of one arrow is the kernel of the next arrow. Thus, from (11), the first arrow is the image, and it is 0 since 0 maps only to itself in $M \otimes \mathbb{Q}$. From this, kernel of the map $M \otimes \mathbb{Q} \to M' \otimes \mathbb{Q}$ (the middle arrow) is equal to 0 also. This gives us that $M \otimes \mathbb{Q} \to M' \otimes \mathbb{Q}$ is injective. Additionally, the last arrow is the kernel of the map $M' \otimes \mathbb{Q} \to 0$. Here, the kernel is everything, since everything maps to 0. Thus, the middle arrow is now the image of the map $M \otimes \mathbb{Q} \to M' \otimes \mathbb{Q}$, which is everything following from the kernel. From this, the map $M \otimes \mathbb{Q} \to M' \otimes \mathbb{Q}$ is surjective. Since we have shown both injectivitty and surjectivity,

$$M \otimes \mathbb{Q} \simeq M' \otimes \mathbb{Q}. \tag{43}$$

Thus, given $M \simeq \mathbb{Z}^n \oplus F$ and $M' \simeq \mathbb{Z}^n \oplus F'$ where F and F' are finite abelian groups, M and M' have the same rank.

$\Leftarrow$

Now, let us assume that M and M' have the same rank. Once again, take the tensor product of the direct sequence considered above:

$$0 \otimes \mathbb{Q} \to M \otimes \mathbb{Q} \to M' \otimes \mathbb{Q} \to (M'/M) \otimes \mathbb{Q} \to 0 \tag{44}$$

Since M and M' have the same rank, $M \otimes \mathbb{Q} \simeq M' \otimes \mathbb{Q}$. Due to this isomorphism, we get that the map is both surjective and injective. Thus, the map has kernel=0 and image=everything. This gives us that the next arrow, the map $M' \otimes \mathbb{Q} \to (M'/M) \otimes \mathbb{Q}$, has kernel=everything, so everything maps to 0.

Therefore, $(M'/M) \otimes \mathbb{Q} = 0$. This means that the rank of (M'/M) is 0, which shows us that M'/M is finite. Thus, assuming that M and M' have the same rank, we have that the map i is of finite index.

□

CHAPTER 16

Ramification in $\mathbb{Z}[\zeta_p]$

by Camilo Bermudez

Let p be a prime in $\mathbb{Z}$, and let R be a $\mathbb{Z}$-algebra. We say that p is **ramified** in R if $R/(p)$ if it contains a nilpotent element: there exists $\alpha \in R, k \in \mathbb{N}$ such that $\alpha^k = 0$ but $\alpha \neq 0$. Otherwise, we say that p is unramified in R.

1. Part One:

Claim: if $m = \prod_{i=1}^{n} p_i^{e_i}$ then $\mathbb{Z}[\zeta_m] = \bigotimes_{i=1}^{n} \mathbb{Z}[\zeta_{p_i^{e_i}}]$.

Proof: The way I will prove this assertion is by showing that there exists a map of inclusion of subrings from right to left and I will show that this map is trivial. We will use the universal property of tensor to show that there exists an n-linear map from the tensor of subrings to the larger ring $\mathbb{Z}[\zeta_m]$. However, first we have to show that each of the $\mathbb{Z}[\zeta_{p_i^e}]$ is a subring of $\mathbb{Z}[\zeta_m]$.

In order to show this, we must remind ourselves that $\mathbb{Z}[\zeta_m]$ is isomorphic to $\mathbb{Z}[x]/\Phi_m$, the ring of polynomials in $\mathbb{Z}$ modded out by the minimal polynomial of ζ_m. Now, in $\mathbb{Z}[\zeta_m]$, we are adjoining all the roots of the minimal polynomial of ζ_m. Any subring of the form $\mathbb{Z}[\zeta_{q_i^{e_i}}]$ where $q|m$, will have all the roots of the minimal polynomial of $\zeta_{q_i^{e_i}}$, which are, of course roots of the minimal polynomial of ζ_m. In other words, the roots in each subring are all roots of the same polynomial Φ_m. Note that these will not account for the primitive m^{th} roots of unity, so we will have to account for these later.

Now we have to define the map between these two rings. As mentioned before, we can use the universal property of the tensor product to define an n-linear map from the tensor to the larger ring. This map is defined by sending a tuple of elements in each subring of the tensor to their product.

$$\iota : \bigotimes_{i=1}^{n} \mathbb{Z}[\zeta_{p_i^{e_i}}] \longrightarrow \mathbb{Z}[\zeta_m]$$
$$(\zeta_{q_1^{e_1}}, \zeta_{q_2^{e_2}}, ..., \zeta_{q_i^{e_i}}) \longmapsto \zeta_{q_1^{e_1}} * \zeta_{q_2^{e_2}} * ... * \zeta_{q_i^{e_i}}.$$

Now we just have to account for all the primitve m^{th} roots of unity, which are not in the subrings. We can show that multiplying two primitive roots of unity will, in turn, give another primitive root of unity. Take for example $m = ab$, for a,b relatively prime. Then we want to show that, $\zeta_a * \zeta_b = \zeta_m$. In other words, if $(\zeta_a * \zeta_b)^n = 1$ for $n < m$, then n=m. We can show this by applying the division algorithm on n.

We begin by dividing n by a and get n=aq+r, so the above now looks: $(\zeta_a * \zeta_b)^{aq+r} = 1$. We can separate this and get $(\zeta_a^{aq} * \zeta_a^r * \zeta_b^{aq+r}) = 1$. The first term will become one, since

it is raised to the power of a multiple of a, and now we can raise everything to the power of be and get $(1 * \zeta_a^{rb} * \zeta_b^{aqb} * \zeta_b^{br}) = 1$. Again, we see that the last two terms will become 1, since they are raised to the power of a multiple of b, which leaves us with $\zeta_a^{rb} = 1$, which means that $a|(rb)$. This leaves two cases: Either $a|b$ or $a|r$. The first case is impossible because a and b are relatively prime. Therefore, $a|r$. This means that n is a multiple of a. By symmetry, we could also show that n is a multiple of b. Now, since $a|n$ and $b|n$, then $m|n$. We know then that $\zeta_a * \zeta_b$ is an m^{th} primitive root of unity, as m is the smallest possible number (i.e. the product of a and b) such that $(\zeta_a * \zeta_b)^m = 1$.

Now that we have shown that the map described above exists and is well defined, we want to show that the inverse to this map exists as well. We will define this map as

$$\tau : \mathbb{Z}[\zeta_m] \longrightarrow \bigotimes_{i=1}^{n} \mathbb{Z}[\zeta_{p_i^{e_i}}]$$
$$\zeta_m \longmapsto \zeta_{q_1} \otimes \zeta_{q_2} \otimes ... \otimes \zeta_{q_m}$$

This map will send the m^{th} root of unity to the tensor of factors-of-m roots of unity. First, we need to check that ζ_m is, in fact, a primitive root of unity. Consider $m = a * b$ for a,b relatively prime. If we raise ζ_m to the m^{th} power, then we get $\zeta_m^{a*b} = 1$. We want to make sure that this is not a k^{th} root of unity, for any $k < a$. We can show this simply by stating that if such k exists, then ζ_m^{b*k} would not be a primite m^{th} root of unity but a primitive bk^{th} root of unity, which is not what we want. Thus, the prime factorization of m determines that ζ_m will be a primitive m^{th} root of unity.

Lastly, we want to check that this inverse map is surjective. Again, consider $m = a * b$ for a,b relatively prime. Then the map will send $\zeta_m \mapsto \zeta_a \otimes \zeta_b$. We want to show that we can generate the entire tensor of subrings from this map. We can do this by taking $(\zeta_a \otimes \zeta_b)^a = (1 \otimes \zeta_b^a)$ from this we can generate the integers with $(1 \otimes 1)$ and the entire subring $\mathbb{Z}[\zeta_b]$ with $(1 \otimes \zeta_b^a)$ by taking powers of ζ_b. Likewise, we can raise the original $(\zeta_a \otimes \zeta_b)^a$ and generate the subring $\mathbb{Z}[\zeta_a]$. Thus in the case of a finite number of prime factors of m, we can generate each of the subrings systematically from the tensor of the factors-of-m roots of unity.

Since we have shown that there exists a well-defined map between these two rings and it contains an inverse, then this map is a bijection. Therefore, this is an isomorphism of rings. We can now consider these two to be *equal* as rings.

2. Part Two:

Claim: Let q be a prime. p is unramified in $\mathbb{Z}[\zeta_{q^k}]$ if and only if $p \neq q$.

Proof: The statement above is equivalent to showing that the m^{th} cyclotomic polynomial is separable. In other words, p is unramified in the smallest possible field that contains all the m^{th} roots of unity. Recall that we are now in characteristic p where, according to the definition of unramified, there should be no nilpotents.

First, lets look at our ring of interest $\mathbb{Z}[\zeta_{q^k}]$ which in characteristic p is equal to the finite field $\mathbb{F}_p[\zeta_{q^k}] \cong \mathbb{F}_p[x]/\Phi_{q^k}$, where Φ_{q^k} is the minimal polynomial of ζ_{q^k}. We know that $\Phi_{q^k} = \prod_{i=1}^{k} f_i(x)$ where each $f_i(x)$ is an irriducible factor of the minimal polynomial. We can use the Chinese Remainder Theorem to get a cartesian product of fields:

$$\mathbb{F}_p[x]/\Phi_{q^k} = \mathbb{F}_p[x]/f_1(x) \times ... \times \mathbb{F}_p[x]/f_k(x)$$

Now we can check that the cartesian product has no nilpotents. Take $(a_1, a_2, ...a_k)^l = 0$ for some $l \epsilon \mathbb{N}$ and a in each of the fields described above. Since the cartesian product is a k-linear map this is equivalent to $(a_1^l, a_2^l, ...a_k^l) = 0$. This means that each of the elements in the cartesian product are $a_i^l = 0$. Since fields have no nilpotents, then this implies that $a_i = 0$. Thus, none of the fields in the cartesian product has a nilpotent element, which means that the original ring will not have any nilpotents.

Now we just have to check the case where $p = q$. Remember that since we are in characteristic p, we can use the Bionomial Theorem to show that the polynomial in $\mathbb{Z}$, $(x^{q^k} - 1) = (x-1)^{q^k}$. Now when we adjoin a root of this polynomial, α, we get $(\alpha - 1)^{q^k} = (\alpha - 1)^{p^k} = 0$. However, we know that $(\alpha - 1) \neq 0$ because $\alpha \neq 1$, since it was adjoined to $\mathbb{Z}$. Thus, $(\alpha - 1)$ must be a nilpotent in this ring and p will be ramified.

3. Part Three:

Claim: p is unramified in $\mathbb{Z}[\zeta_m]$ if and only if $p \nmid m$.

Proof: This is a more general statement than what was proven in Part Two. Recall that $m = \prod_{i=1}^{n} p_i$, so as shown in Part One, we can decompose the ring $\mathbb{Z}[\zeta_m]$ into the tensor of subrings. However, now we want to see how this behaves in characteristic p, so we get:

$$\mathbb{F}_p[x]/\Phi_m = \mathbb{F}_p[x]/\Phi_{q_1} \otimes ... \otimes \mathbb{F}_p[x]/\Phi_{q_n}$$

As shown in Part One, if $p|m$, then one of the subrings in the tensor will be of the form $\mathbb{F}_p[x]/\Phi_{p_1}$. We know from Part Two that the subring of the p^{th} root of unity in characteristic p will have a nilpotent element. Therefore, if there is a nilpotent element in the tensor, then there will be a nilpotent element in the larger ring, since these two are isomorphic. This is easily shown by the map that takes a tuple of elements in the tensor to their product in the larger ring.

If $p \nmid m$, then none of the elements would have nilpotents and p would be unramified in $\mathbb{Z}[\zeta_m]$.

CHAPTER 17

Algebras of Dimension 2

by David Fertig

1. Algebras of Dimension 2

Let k be a field. Let A be a (commutative!) k-algebra.

(1) Prove that if $\dim_k A < \infty$ then A is an integral domain if and only if A is a field.
(2) Prove that if $\dim_k(A) = 2$, then
   (a) If A is a field, A is either generated by the square root of an element α in k or, if the characteristic of k is 2, by an Artin-Schreier root $\wp^{-1}(\alpha)$ for some $\alpha \in k$.
   (b) Show that if A is not a field, then either $A = k \times k$ or $A = k[t]/t^2$.

1.1. Proof of 1. $\Leftarrow$ If A is a field, A is an integral domain.
$\Rightarrow$ Using the Rank-Nullity Theorem

(1) Consider a non-zero $y \in A$.
(2) $T : A \Leftrightarrow A$ such that $Tx = yx$ $x \in A$.
(3) By Rank-Nullity Theorem, $dim(ker(T)) + dim(im(T)) = dim(A)$.
(4) $dim(im(T)) = dim(A)$ because $T : A \Leftrightarrow A$ which implies $dim(ker(T)) = 0$.
(5) This means that T is surjective with a trivial kernel, which implies that there exists $z \in A$ such that $zy = 1$, so every $y \in A$ is invertible.
(6) So A being an integral domain implies A is a field.

1.2. Proof of 2a.

(1) If $\sqrt{\alpha} \in A$, $\sqrt{\alpha} \notin k$, and $\alpha \in k$, $k[\sqrt{\alpha}]$ is a two dimensional k-algebra with a basis $[1, \sqrt{\alpha}]$.
(2) $A = k[\sqrt{\alpha}] = [x + (y * \sqrt{\alpha}) \mid \forall x, y \in k]$.
(3) $a, b \in A$. If $x, y \in K$ and $x * y = 0$, $\Rightarrow x$ or $y = 0$.
(4) $\Rightarrow A$ is an integral domain $\Rightarrow A$ field by 17.1.
(5) All elements of A have cardinality = 2.
(6) By 11.3, all fields with the same cardinality are isomorphic. $\Rightarrow$ all fields A when K has characteristic > 2 are isomorphic to $k[\sqrt{\alpha}]$ as shown above.
(7) If you attach more than one root to k, $dim_k A > 2$.
(8) If $char(k) = 2$ meaning $1 + 1 = 0$ in k, you must attach the Artin-Schreier root as described in problem 9.

(9) $A = k[X]/[X^2 - X - \alpha]]$ where $\wp^{-1}(\alpha')$ is the solution to $X^2 - X - \alpha = 0$, so $A = k[(\wp^{-1}(\alpha'))]$.
(10) $X^2 - X - \alpha$ is irreducible in k when $char(k) = 2$, so A is a field.
(11) Again by 11.3, all fields with the same cardinality are isomorphic, so all algebras over k of $dim_k A = 2$ where $char(k) = 2$ are isomorphic to $A = k[(\wp^{-1}(\alpha'))]$.

1.3. Proof of 2b.

(1) $A = k \times k = [a \times b \mid \forall a, b \in k]$ and $A = k[t]/t^2 = [a + bt \mid \forall a, b \in k]$.
(2) $[(0,1),(1,0)] \in k \times k$, and $(0,1) \times (1,0) = (0,0) \Rightarrow k \times k$ is not a field.
(3) $(0 + 1t) \in k[t]/t^2$ and $(0 + 1t) \times (0 + 1t) = 0 \Rightarrow k[t]/t^2$ is not a field.
(4) Assume f(t) is a quadratic function with both roots $a, b \in k$, $A = k[t]/f(t)$ is not a field because $[(t - a), (t - b)] \in k[t]/t^2$ and $(t - a) \times (t - b) = 0 \in k[t]/f(t)]$.
(5) $k[t]/f(t) \cong k[t]/t^2 \Rightarrow$ all non-field A with $dim_k A = 2$ take are equivalent to the forms $k \times k$ or $k[t]/t^2$.

CHAPTER 18

Quadratic Residues

by Samuel Charles Passaglia

Let p be a prime number. We say an integer m is a square mod p if and only if there is an integer n such that $m \equiv n^2 \pmod{p}$. We define the **quadratic residue symbol**

$$\left(\frac{m}{p}\right) =_{\text{def}} \begin{cases} 1 & \text{if } m \text{ is a square mod } p \\ 0 & \text{if } p|m \\ -1 & \text{otherwise} \end{cases} \tag{45}$$

(1) Prove that

$$\left(\frac{m}{p}\right) = m^{\frac{p-1}{2}} \pmod{p}. \tag{46}$$

Proof. Note p should be an odd prime. $\left(\frac{m}{p}\right) = 0 \Leftrightarrow m = n \cdot p$ for some $n \in \mathbb{F}_p^\times \Leftrightarrow m^{\frac{(p-1)}{2}} \pmod{p} = (n \cdot p)^{\frac{(p-1)}{2}} \pmod{p} = (n)^{\frac{p-1}{2}} \pmod{p} \cdot (p)^{\frac{(p-1)}{2}} \pmod{p} = 0 \pmod{p}$.

Theorem 22 (Fermat's Little Theorem). *For p prime, $m \in \mathbb{F}_p^\times$,*

$$m^p \equiv m \pmod{p}. \tag{47}$$

Hence:

$$m^{p-1} \equiv 1 \pmod{p}. \tag{48}$$

$\mathbb{F}_p^\times$ is a group under multiplication, thus every element to the power of the order of the group is equal to 1. Since the order of $\mathbb{F}_p^\times$ is $(p-1)$, then we get the result above.

$m^{p-1} \equiv 1 \pmod{p} \Leftrightarrow (m^{\frac{p-1}{2}} + 1) \cdot (m^{\frac{p-1}{2}} - 1) \equiv 0 \pmod{p}$. Hence:

$$m^{\frac{p-1}{2}} \equiv 1 \text{ or } -1 \pmod{p}. \tag{49}$$

Thus we are reduced to compute

$$\left(\frac{m}{p}\right) = 1 \Leftrightarrow m^{\frac{p-1}{2}} \equiv 1 \pmod{p} \tag{50}$$

"⇒" Want to show: If $\left(\frac{m}{p}\right) = 1$ then $m^{\frac{p-1}{2}} \equiv 1 \pmod{p}$

$\left(\frac{m}{p}\right) = 1 \Rightarrow m \equiv n^2 \pmod{p} \Rightarrow m^{\frac{p-1}{2}} \equiv n^{p-1} \pmod{p} \equiv 1 \pmod{p}$ (By Theorem 1)

"⇐" Want to show: If $m^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ then $\left(\frac{m}{p}\right) = 1$
Recall from Project 10 that the multiplicative group of a finite field is cyclic. Thus $m = a^j$ for some j, where a is the generator of $\mathbb{F}_p^\times$. Hence $a^{\frac{j\cdot(p-1)}{2}} \equiv 1 \pmod{p}$. Given that p-1 is the order of $\mathbb{F}_p^\times$, $(p-1)|(j \cdot \frac{p-1}{2})$. Thus, j is even. Now consider the element $a^{\frac{j}{2}}$ of $\mathbb{F}_p^\times$. $(a^{\frac{j}{2}})^2 = a^j = m$ Thus, m is a quadratic residue mod p. □

(2) Prove that the map

$$\kappa_p : \mathbb{F}_p^\times \to \{\pm 1\} \tag{51}$$

given by

$$\kappa_p(m) =_{\text{def}} \left(\frac{m}{p}\right) \tag{52}$$

is a group homomorphism. Prove that in fact it is the only non-trivial such homomorphism.

Proof. We need to show that $\kappa_p(a \cdot b) = \kappa_p(a) \cdot \kappa_p(b)$
$\kappa_p(a) \cdot \kappa_p(b) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p} \cdot b^{\frac{p-1}{2}} \pmod{p} \equiv (a \cdot b)^{\frac{p-1}{2}} \pmod{p} \equiv \left(\frac{a\cdot b}{p}\right) = \kappa_p(a \cdot b)$
To show homomorphism is unique: $\mathbb{F}_p^\times$ is a cyclic group under multiplication (from Project 10), hence every element can be expressed as a product of the group generator. Thus, all homomorphisms from $\mathbb{F}_p^\times$ are uniquely determined by the image of the group generator. If the group generator maps to 1, clearly the homomorphism is trivial. Otherwise, the group generator maps to -1, in which case we have a non-trivial homomorphism, this one. Note that the generator g is never a quadratic residue for odd p (for even p, it trivially is a quadratic residue). For odd p, g being a quadratic residue implies $g^{\frac{(p-1)}{2}} = 1$, which contradicts that the order of the multiplicative group is $p - 1$. □

(3) Prove that, if p is an odd prime, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ and $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. (Hint: for -1, use cyclicity of $\mathbb{F}_p^\times$. For 2, let ζ be an eighth root of unity. Calculate the powers of $\zeta + \zeta^{-1}$.

Proof. For -1, we see that $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$. Since p is odd, $(-1)^{\frac{p-1}{2}}$ is either 1 or -1. Thus, the mod never enters play, and we get that $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.
For -2, consider ζ a primitive eighth root of unity in $\mathbb{F}_p^\times[\zeta]$. This is a commutative ring, and we define the usual modular equivalence relation on it. $\zeta^8 - 1 = 0 \implies (\zeta^4 + 1) \cdot (\zeta^4 - 1) = 0$. ζ primitive implies $(\zeta^4 + 1) = 0$. Hence $\zeta^2 + \zeta^{-2} = 0$ and therefore by completing the square we get that $(\zeta + \zeta^{-1})^2 = 2$. By part 1, this

$\implies \left(\frac{2}{p}\right) \equiv (\zeta + \zeta^{-1})^{(p-1)} \mod p$.

Recall the binomial theorem: $(x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^{p-i} y^i$ where $\binom{p}{i} = \frac{p!}{i!(p-i)!}$. The first and last coefficients of the expansion are clearly 1. For all other terms the factorial of a prime is divided by the product of two factorials of lesser numbers. Therefore $\frac{p!}{i!(p-i)!}$ will be a multiple of p, and therefore $0 \mod p$, unless $i = 1$ or p.

Thus $(\zeta + \zeta^{-1})^p \equiv \left(\frac{2}{p}\right) \cdot (\zeta + \zeta^{-1}) \mod p$ implies by the binomial theorem above the following useful result:

$$(\zeta^p + \zeta^{-p}) \equiv \left(\frac{2}{p}\right) \cdot (\zeta + \zeta^{-1}) \mod p \tag{53}$$

Now since ζ is a primitive eighth root of unity, $\zeta^p = \zeta^{p \pmod 8}$. Thus since p is an odd prime, we must consider four cases, $p \equiv 1, 3, 5, 7 \pmod 8$, in order to reduce the above equation into a form in which ζ does not appear.

Case 1: $p \equiv 1 \pmod 8$.

$(\zeta+\zeta^{-1}) = \left(\frac{2}{p}\right)\cdot(\zeta+\zeta^{-1}) \implies (\zeta+\zeta^{-1})^2 = \left(\frac{2}{p}\right)\cdot(\zeta+\zeta^{-1})^2 \implies 2 = \left(\frac{2}{p}\right)\cdot 2 \implies \left(\frac{2}{p}\right) = 1$.

Case 2: $p \equiv -1 \pmod 8$.

$(\zeta^{-1} + \zeta^1) = \left(\frac{2}{p}\right) \cdot (\zeta + \zeta^{-1}) \implies \left(\frac{2}{p}\right) = 1$

Case 3: $p \equiv 3 \pmod 8$.

$(\zeta^3 + \zeta^{-3}) = \left(\frac{2}{p}\right) \cdot (\zeta + \zeta^{-1})$. But consider the following: $(\zeta^3 + \zeta^{-3}) = (\zeta^4 \cdot \zeta^{-1} + \zeta^1\zeta^{-4}) = \zeta^4 \cdot \zeta^4(\zeta^4 \cdot \zeta^{-1} + \zeta^1\zeta^{-4}) = \zeta^4(\zeta^{-1} + \zeta^1)$. Recall from above that $\zeta^4 = -1$, so get $(\zeta^3 + \zeta^{-3}) = -1 \cdot (\zeta^{-1} + \zeta^1)$ and thus $\left(\frac{2}{p}\right) = -1$.

Case 4: $p \equiv -3 \pmod 8$.

Both by symmetry with case 3 and analogy to the relationship between case 2 and case 1, it is clear that $\left(\frac{2}{p}\right) = -1$.

Hence it is clear that $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ is correct because it gives the answers above in all cases of p.

□

CHAPTER 19

Splitting of Primes in Quadratic Number Rings

by Jose Maria Barrero

1. Problem statement

Let p and q be odd primes. Prove that

$$\mathbb{Z}\left[\sqrt{(-1)^{(p-1)/2}p}\right]/(q) = \begin{cases} \mathbb{F}_q \oplus \mathbb{F}_q & \text{if and only if } \left(\frac{(-1)^{(p-1)/2}p}{q}\right) = 1, \\ \mathbb{F}_{q^2} & \text{if and only if } \left(\frac{(-1)^{(p-1)/2}p}{q}\right) = -1, \text{ and} \\ \mathbb{F}_q[x]/(x^2) & \text{if and only if } \left(\frac{(-1)^{(p-1)/2}p}{q}\right) = 0. \end{cases} \tag{54}$$

In the first case we say q **splits**, in the second case, it **stays inert**, and in the third case, it **ramifies**.

2. The nature of $\mathbb{Z}\left[\sqrt{(-1)^{(p-1)/2}p}\right]/(q)$

Our first step to proving the claims is to understand and explore the nature of the ring we are working with.

For notational simplicity, define $(-1)^{(p-1)/2}p \equiv \gamma$ so that we are working with $\mathbb{Z}\left[\sqrt{\gamma}\right]/(q)$. Note that γ always corresponds to an element of the field $\mathbb{F}_q$, since it is simply an odd prime number multiplied by plus or minus one, so it can always be mapped to a residue class in $\mathbb{F}_q$.

- *Lemma*: $\mathbb{Z}\left[\sqrt{\gamma}\right]/(q) = \mathbb{F}_q\left[x\right]/(x^2-\gamma)$

proof

Let $R = \mathbb{Z}\left[\sqrt{\gamma}\right]$ so that $\mathbb{Z}\left[\sqrt{\gamma}\right]/(q) = R/(q)$.

However, note that R itself can be realized as

$$R = \mathbb{Z}\left[x\right]/(x^2-\gamma),$$

that is, by creating a quotient ring from the polynomial ring $\mathbb{Z}\left[x\right]$ over the principal ideal generated by $f(x) = x^2 - \gamma$. This procedure effectively adjoins a square root of γ to $\mathbb{Z}$, creating a two-dimensional algebra over $\mathbb{Z}$.

Therefore, $R/(q)$ can be realized by quotienting $\mathbb{Z}\left[x\right]$ successively by $(x^2-\gamma)$ and (q):

$$R/(q) = \mathbb{Z}\left[\sqrt{\gamma}\right]/(q) = \frac{\mathbb{Z}\left[x\right]/(x^2-\gamma)}{(q)} \tag{55}$$

Note that quotienting by (q) in $\mathbb{Z}[x]$ is a nontrivial operation, since q is a prime, so it is therefore not a unit. It acts on the polynomial ring (and on R) by sending the coefficient of each term to its residue class *mod* q since $ax^n = mqx^n + [a]_q x^n \mapsto [a]_q x^n$ when quotienting by (q).

This double quotienting is equivalent to quotienting by the principal ideal generated by these two elements together : $(q, x^2 - \gamma)$. Indeed,

$$(q, x^2 - \gamma) = \{qr_1 + (x^2 - \gamma)r_2 \mid r_1, r_2 \in \mathbb{Z}[x]\}, \tag{56}$$

so quotienting by $(x^2-\gamma)$ sends an element $qr_1+(x^2-\gamma)r_2 \mapsto qr_1$ by the division algorithm, and then quotienting by (q) sends it to 0. So we have that quotienting by both ideals succesively annihilates exactly those elements in the principal ideal $(q, x^2 - \gamma)$.

More importantly, this result implies that the double quotienting above is equivalent to quotienting succesively in the other order, first by (q) and then, since all coefficients are now residues *mod* q, by $(x^2 - [\gamma]_p)$ to get that

$$\mathbb{Z}[\sqrt{\gamma}]/(q) = \frac{\frac{\mathbb{Z}}{(q)}[x]}{(x^2 - [\gamma]_p)} \tag{57}$$

or, equivalently, since q is a prime:

$$\mathbb{Z}[\sqrt{\gamma}]/(q) = \mathbb{F}_q[x]/(x^2 - [\gamma]_p). \tag{58}$$

□

Thus, we can characterize $\mathbb{Z}\left[\sqrt{\gamma}\right]/(q)$ as the quotient of a polynomial ring over a field, allowing us to use some of the important results developed earlier in the semester.

3. Rethinking quadratic residues

By definition, $(\frac{p}{q}) = 1$ if and only if there exist an integer n such that $n^2 \equiv p \pmod{q}$. That is, if $n^2 - p \equiv 0 \pmod{q}$ or equivalently if the polynomial $f(x) = x^2 - [p]_q$ has a nonzero root in $\mathbb{F}_q$, where $[p]_q$ denotes the residue class of p in $\mathbb{F}_q$.

Similarly $(\frac{p}{q}) = -1$ if there is no integer n satisfying $n^2 \equiv p \pmod{q}$. In other words, if $f(x) = x^2 - [p]_q$ is irreducible over $\mathbb{F}_q$.

Finally, $(\frac{p}{q}) = 0$ if q divides p, which is to say that $p \equiv 0 \pmod{q}$.

Therefore we can group the results into the following lemma:

- $(\frac{p}{q}) = 1$ if and only if $[p]_q \neq 0$ and the polynomial $f(x) = x^2 - [p]_q$ is not irreducible over $\mathbb{F}_q$.
- $(\frac{p}{q}) = -1$ if and only if $[p]_q \neq 0$ and the polynomial $f(x) = x^2 - [p]_q$ is irreducible over $\mathbb{F}_q$.
- $(\frac{p}{q}) = 0$ if and only if $[p]_q = 0$.

4. Proof of the theorem

In any of the three cases outlined in the problem, $\mathbb{Z}\left[\sqrt{\gamma}\right]/(q) = \mathbb{F}_q[x]/(x^2 - [\gamma]_q)$ is a two-dimensional vector space over $\mathbb{F}_q$, but is slightly different in each.

(1) $\mathbb{F}_q[x]/(x^2 - [\gamma]_q) = \mathbb{F}_q \oplus \mathbb{F}_q$ if and only if $\left(\frac{\gamma}{q}\right) = 1$

proof

- Consider the polynomial $f(x) = x^2 - [\gamma]_p$ in $\mathbb{F}_q[x]$ and let $[\gamma]_q \neq 0$. By the above lemma, $(\frac{\gamma}{q}) = 1$ implies that $f(x)$ is not irreducible over $\mathbb{F}_q$.

  Then, by an earlier problem set, the quotient ring $\mathbb{F}_q[x]/(x^2 - [\gamma]_q)$ will be a two-dimensional vector space over $\mathbb{F}_q$ (since $f(x)$ is a quadratic polynomial), but *not* a field. Then we have that the quotient is simply the direct sum $\mathbb{F}_q \oplus \mathbb{F}_q$.
- Conversely, if we know that the quotient $\mathbb{F}_q[x]/(x^2 - [\gamma]_q) = \mathbb{F}_q \oplus \mathbb{F}_q$, is not a field, and $x^2 - [\gamma]_q \neq x^2$ in $\mathbb{F}_q[x]$, it must be that $f(x)$ is not irreducible over $\mathbb{F}_q$, and thus that $(\frac{\gamma}{q}) = 1$.

(2) $\mathbb{F}_q[x]/(x^2 - [\gamma]_q) = \mathbb{F}_{q^2}$ if and only if $\left(\frac{\gamma}{q}\right) = -1$

proof

- If $\left(\frac{\gamma}{q}\right) = -1$, the polynomial $f(x) = x^2 - [\gamma]_p$ does not have a root over $\mathbb{F}_q$ and is therefore irreducible over that field. This implies that the quotient $\mathbb{F}_q[x]/(x^2 - [\gamma]_p)$ is a field. Also, it will be a two-dimensional vector space over $\mathbb{F}_q$, and therefore $\mathbb{F}_q[x]/(x^2 - [\gamma]_q)$ will be in bijection with $\mathbb{F}_q \times \mathbb{F}_q$. This last fact implies that $\mathbb{F}_q[x]/(x^2 - [\gamma]_q)$ has exactly q^2 elements, and since it is a field we get the result that $\mathbb{F}_q[x]/(x^2 - [\gamma]_q) = \mathbb{F}_{q^2}$.
- Conversely, if we know that the quotient $\mathbb{F}_q[x]/(x^2 - [\gamma]_q) = \mathbb{F}_{q^2}$, a field, it must be that the polynomial $f(x)$ defined above is irreducible over $\mathbb{F}_q$ and therefore that $\left(\frac{\gamma}{q}\right) = -1$.

(3) $\mathbb{F}_q[x]/(x^2 - [\gamma]_q) = \mathbb{F}_q/(x^2)$ if and only if $\left(\frac{\gamma}{q}\right) = 0$

proof

- $\left(\frac{\gamma}{q}\right) = 0$ implies that $\gamma \equiv 0 \pmod{q}$. Therefore, the polynomial $f(x) = x^2 - [\gamma]_q$ is actually $f(x) = x^2$. Immediately we get the result that $\mathbb{F}_q[x]/(x^2 - \gamma) = \mathbb{F}_q[x]/(x^2)$.
- On the other hand, if we know that $\mathbb{F}_q[x]/(x^2 - [\gamma]_q) = \mathbb{F}_q[x]/(x^2)$, (i.e. that in $\mathbb{F}_q[x]$, $f(x) = x^2$) then we have that $\gamma \equiv 0 \pmod{q}$, and therefore that q divides γ, implying that $\left(\frac{\gamma}{q}\right) = 0$.

□

CHAPTER 20

Totally ramified extensions

by David Costigan

(1) Prove that $\mathbb{Z}[\zeta_{p^k}]/(p) = (\mathbb{Z}/p)[t]/\left(t^{\dim_{\mathbb{Q}} \mathbb{Z}[\zeta_{p^k}] \otimes_{\mathbb{Z}} \mathbb{Q}}\right)$. We say that $\mathbb{Z}[\zeta_{p^k}]$ is **totally ramified** at p.

First, see that $\mathbb{Z}[\zeta_{p^k}] \cong \mathbb{Z}[x]/(\Xi_{p^k})$, since ζ_{p^k} is a primitive $p^{k\text{-th}}$ root of unity and Ξ_{p^k} is the unique irreducible polynomial whose roots are the $p^{k\text{-th}}$ roots of unity (i.e., Ξ_{p^k} is the $p^{k\text{-th}}$ cyclotomic polynomial). Ξ_{p^k} is defined recursively as $\Xi_{p^k} = \dfrac{x^{p^k} - 1}{\prod\limits_{\substack{d|p^k \\ d \neq p^k}} \Xi_d}$. We also have that $\Xi_1 = x - 1$ by definition. Next, when we mod out by the ideal generated by p, we make the characteristic of the ring equal to p. We can see that, in characteristic p, $\Xi_{p^k} = \dfrac{(x-1)^{p^k}}{\prod\limits_{\substack{d|p^k \\ d \neq p^k}} \Xi_d}$. Then, in the product $\prod\limits_{\substack{d|p^k \\ d \neq p^k}} \Xi_d$, there are k terms, since the divisors of p^k are $(1, p, \ldots, p^{k-1})$. We can then write the denominator as $\Xi_1 \cdot \Xi_p \cdots \Xi_{p^{k-1}}$. Using the recursive definition of the cyclotomic polynomial, we can rewrite the denominator as $(x-1) \cdot \dfrac{x^p - 1}{x - 1} \cdot \dfrac{x^{p^2} - 1}{(x-1)\dfrac{(x^p - 1)}{x - 1}} \cdots$. Since we are in characteristic p, we see that $x^{p^n} - 1 = (x-1)^{p^n}$ for any $n \in \mathbb{N}$, so in characteristic p our denominator becomes $(x-1) \cdot (x-1)^{p-1} \cdot (x-1)^{p^2-p} \cdots (x-1)^{p^{k-1}-p^{k-2}}$, which collapses to $(x-1)^{p^{k-1}}$. So, we get that, in characteristic p, $\Xi_{p^k} = \dfrac{(x-1)^{p^k}}{(x-1)^{p^{k-1}}} = (x-1)^{p^k - p^{k-1}}$. From project #12, we know that $\phi(p^k)$ is equal to $p^k - p^{k-1}$, where ϕ is Euler's totient function. So we can write $(x-1)^{p^k - p^{k-1}} = (x-1)^{\phi(p^k)}$, and we can write $\mathbb{Z}[\zeta_{p^k}] \cong \mathbb{F}_p[x]/(x-1)^{\phi(p^k)} \cong (\mathbb{Z}/p)[x]/(x-1)^{\phi(p^k)}$. We can do a change of variable

of $x-1$ to t and we get $(\mathbb{Z}/p)[t]/(t)^{\phi(p^k)}$. Now, we note that the rank of a module $\mathbb{Z}[\zeta_{p^k}]$ over a ring $\mathbb{Z}$ imbeddable in a field $\mathbb{Q}$ is defined to be the dimension of the tensor product $\mathbb{Z}[\zeta_{p^k}] \otimes_{\mathbb{Z}} \mathbb{Q}$ as a vector space over $\mathbb{Q}$. Thus, $\dim_{\mathbb{Q}} \mathbb{Z}[\zeta_{p^k}] \otimes_{\mathbb{Z}} \mathbb{Q}$ is just the rank of the group generated by ζ_{p^k} viewed as a $\mathbb{Z}$-module, which we know is $\phi(p^k)$. Thus, we get that $\mathbb{Z}[\zeta_{p^k}]/(p) = (\mathbb{Z}/p)[t]/\left(t^{\dim_{\mathbb{Q}} \mathbb{Z}[\zeta_{p^k}] \otimes_{\mathbb{Z}} \mathbb{Q}}\right)$.

(2) Any element A of $k[t]/(t^n)$ acts on an n-dimensional vector space V, preserves a filtration $0 = V_0 \subset V_1 \subset V_2 \subset V_3 \subset \ldots \subset V_n = V$ with $dim(V_i/V_{i-1}) = 1$ and such that there exists an $l \in k$ so that A acts on V_i/V_{i-1} by multiplication by l.

We can let $V = k[t]/(t^n)$, and we see that there is a filtration $0 = t^n k[t]/(t^n) \subset t^{n-1}k[t]/(t^n) \ldots \subset tk[t]/(t^n) \subset k[t]/(t^n) = V$. We see that V is an n-dimensional vector, as required, because $k[t]/(t^n)$ can be viewed as an n-dimension vector space over k. We also see that, as we move from left to right in the filtration, the dimension of the subspace increases by 1, so $\dim(V_i/V_{i-1}) = \dim(V_i)$ - $\dim(V_{i-1}) = 1$. Any element $A \in k[t]/(t^n)$ acts on V by regular multiplication, so this property is satisfied. We need only show that A acts on V_i/V_{i-1} by multiplication of a constant $l \in k$. To see this, take any element $A = a_{n-1}t^{n-1} + \ldots + a_1 t + a_0$ and multiply it by any $V_i/V_{i-1} = (t^{n-i}k[t]/(t^n))/(t^{n-i+1}k[t]/(t^n))$. If we multiply A by t^{n-i}, we get $t^{n-i}\cdot(a_{n-1}t^{n-1}+\ldots+a_1t+a_0) = a_{n-1}t^{2n-i-1}+\ldots+a_1t^{n-i+1}+a_0t^{n-i}$. But we see that everything with an exponent greater than or equal to $n-i+1$ gets sent to 0 in V_i/V_{i+1}, so the only term that remains is a_0t^{n-i}. Thus, A acts on V_i/V_{i+1} by multiplication of the constant term a_0 in A, and since $a_0 \in k$, we can let $a_0 = l$ to satisfy the proposition. This action also preserves the filtration, since multiplication by an element of k cannot change the dimension of V_i/V_{i-1}.

(3) Let m be a squarefree number. At which primes is $\mathcal{O}_m$ ramified? Prove that $\mathcal{O}_m$ ramifies only at p if and only if $m = (-1)^{(p-1)/2}p$.

From problem #5, we can write $\mathcal{O}_m = \mathbb{Z}[\alpha]$, where $\alpha = \frac{1+\sqrt{m}}{2}$ if $m \equiv 1 \pmod 4$ and $\sqrt{m}$ otherwise. From the definition of ramification, $\mathcal{O}_m$ ramifies at p if $\mathcal{O}_m/(p)$ has a non-zero nilpotent element. We can write $\mathcal{O}_m = \mathbb{Z}[X]/f(x)$, where $f(x)$ is some irreducible quadratic polynomial. $\mathcal{O}_m$ will ramify at p if, in characteristic p, $f(x)$ has a repeated root, i.e., $f(x)$ can be factored into $f(x) = (f_1(x))^2$ in characteristic p, because then there will be a non-zero element in $\mathcal{O}_m/(p)$ that, when squared, will equal 0. Now, take the two possible minimal polynomials of α, which are $X^2 - X + (1-m)/4$ for $m \equiv 1 \pmod 4$ and $X^2 - m$ for $m \not\equiv 1 \pmod 4$. We can factor these polynomials in $\mathbb{F}_p[X]$ as ${f_1}^{e_1} \cdot {f_2}^{e_2}$. From the quadratic formula $-b \pm \frac{\sqrt{b^2-4ac}}{2a}$, we see that a quadratic polynomial has a repeated root iff its discriminant, b^2-4ac, is equal to 0. Thus, $f(x)$ has a repeated root in $\mathbb{F}_p$ if its discriminant is 0 in $\mathbb{F}_p$. So, we take the discriminants of the two polynomials and find that the discriminant of $X^2 - X + (1-m)/4$ is m, and the discriminant of $X^2 - m$ is $4m$. Thus, $\mathcal{O}_m$ ramifies at p if and only if p divides m

when $m \equiv 1 \pmod 4$ and $4m$ when $m \not\equiv 1 \pmod 4$. Since we want $\mathcal{O}_m$ to ramify at exactly one prime, we must have that $m \equiv 1 \pmod 4$, because $2|4m$ for all m, so if $m \not\equiv 1 \pmod 4$ then 2 and p would both ramify in $\mathcal{O}_m$. For $\mathcal{O}_m$ to ramify at only p, we also need $m = \pm p$. Note that m must be square free, so it cannot be the square of a prime. Since some primes are $1 \pmod 4$ and some primes are $3 \pmod 4$, we need to"convert" all of the primes that are $3 \pmod 4$ to ones that are $1 \pmod 4$. We do this by taking $m = (-1)^{(p-1)/2}p$, since, with this value of m, $m \equiv 1 \pmod 4$ for all odd primes p, which follows from Question #18. So $\mathcal{O}_m$ ramifies only at p if and only if $m = (-1)^{(p-1)/2}p$.

(4) Let $R \subseteq \mathcal{O}_m$ be a subring, $R \neq \mathbb{Z}$. Prove that a prime p ramifies in R if and only if p ramifies in $\mathcal{O}_m$ or $p \mid \#\mathcal{O}_m/R$.

First, we see that $R \neq \mathbb{Z}$ because $\mathbb{Z}$ does not ramify at any prime p, since $\mathbb{Z}/(p)$ is a field for any prime p.

Next, from above, we see that if $\mathcal{O}_m$ ramifies at p, then p divides the discriminant of the minimal polynomial $x^2 - x + (1-m)/4$ if $m \equiv 1 \pmod 4$ or $x^2 - m$ when $m \not\equiv 1 \pmod 4$. These discriminants are either m or $4m$. Since $\mathcal{O}_m = \mathbb{Z}[\alpha]$, we can see that subrings of $\mathcal{O}m$ are of the form $l\mathbb{Z}[n\alpha]$, where $n, l \in \mathbb{N}$. This is because subrings must contain the identity element of $\mathcal{O}m$ and be subgroups of $(\mathcal{O}m, +)$. Subgroups of $(\mathcal{O}m, +)$ must be closed under addition, so the only groups of this form are $\mathbb{Z}[n\alpha]$. Since we can make the subring smaller by multiplying the coefficients by a constant, we get that the subrings are $l\mathbb{Z}[n\alpha]$. The minimal polynomials of $l\mathbb{Z}[n\alpha]$ are now either $x^2 - x + (1 - n^2m)/4$ or$x^2 - n^2m$, whose discriminants are either n^2m or $4n^2m$, respectively. Since p divided either m or $4m$, p must also divide n^2m or $4n^2m$, so R ramifies at p.

Next, assume that p does not ramify in $\mathcal{O}_m$. If p divides the order of $\mathcal{O}_m/R$, then $p(a + b\alpha + (R)) = 0$ in $\mathcal{O}_m/R$ for some element $(a + b\alpha)$ in $\mathcal{O}_m$, which means that $pa+pb\alpha$ is 0 in $\mathcal{O}_m/R$, which means that $pa+pb\alpha$ is in R. But since p is prime, and R is a subring that isn't $\mathcal{O}_m$ itself, you can't have $pa + pb\alpha$ as an element of R unless the subring is $Z[np\alpha]$ where np is some multiple of p and n divides b. Then, the minimal polynomial of $Z[np\alpha]$ is no longer either $x^2 - x + (1-m)/4$ or $x^2 - m$, as it was in $\mathcal{O}_m$; it becomes either $x^2 - x + (1 - (np)^2m)/4$ or $x^2 - (np)^2m$. The discriminants of these polynomials are now either $(np)^2m$ or $4(np)^2m$, which means that the minimal polynomial has a repeated root in characteristic p since p divides the discriminant, which means that $Z[np\alpha]$ ramifies at p, as claimed.

CHAPTER 21

Decomposition Theory of Cyclotomic Fields

by Constantin Gumeniță

Let p, q be distinct prime numbers. Recall that $\Gamma_q = \mathrm{Aut}(\mathbb{Q}(\zeta_q))$.

(1) Deduce from Project 10 that Γ_q is cyclic.
(2) Use the orbit-stabilizer theorem to prove that $\mathbb{Z}[\zeta_q]/(p) \cong (\mathbb{F}_{p^\ell})^k$ where $\ell k = q-1$.
(3) Let $G \subseteq \Gamma_q$. Prove that $(\mathbb{Z}[\zeta_q]/(p))^G$, the fixed ring, is of dimension $[\Gamma_q : G]$ over $\mathbb{F}_p$.
(4) Prove that ℓ is the least number such that $q \mid p^\ell - 1$. (Note that this is consistent with the fact that $p^{q-1} \equiv 1 \pmod q$)

Solution:

(1) Deduce from Project 10 that Γ_q is cyclic.

PROOF. In Project 13 we defined $\Gamma_q = \mathrm{Aut}(\mathbb{Q}(\zeta_q)) \cong \mathrm{Aut}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) \cong (\mathbb{Z}/q)^\times$. By Project 10, every finite subgroup of the multiplicative group $k^\times$ of a field k is cyclic. Since $\Gamma_q \cong (\mathbb{Z}/q)^\times$ is the multiplicative subgroup of $\mathbb{Z}/q$, Γ_q is cyclic. □

(2) Use the orbit-stabilizer theorem to prove that $\mathbb{Z}[\zeta_q]/(p) \cong (\mathbb{F}_{p^\ell})^k$ where $\ell k = q-1$.

PROOF. $\mathbb{Z}[\zeta_q] \cong \mathbb{Z}[x]/(\Phi_q(x))$, where $\Phi_q(x) = x^{q-1} + ... + x + 1$ is the minimal polynomial of ζ_q over $\mathbb{Z}[x]$, and concurrently the q-th cyclotomic polynomial. Hence, $\mathbb{Z}[\zeta_q]/(p) \cong (\mathbb{Z}[x]/(\Phi_q(x)))/(p) \cong \mathbb{Z}[x]/(\Phi_q(x), p) \cong (\mathbb{Z}[x]/(p))/(\overline{\Phi_q(x)}) \cong (\mathbb{Z}/p\mathbb{Z}[x])/(\overline{\Phi_q(x)}) \cong \mathbb{F}_p[x]/(\overline{\Phi_q(x)})$ where $\overline{\Phi_q(x)}$ represents the residue class of $\Phi_q(x)$ in $\mathbb{F}_p$.

While $\Phi_q(x)$ is irreducible over $\mathbb{Z}[x]$, $\overline{\Phi_q(x)}$ is not necessarily irreducible over $\mathbb{F}_p[x]$. Let $\overline{\Phi_q(x)}$ factor over $\mathbb{F}_p[x]$ into $\overline{\Phi_q(x)} = \prod_{1 \le i \le k} \overline{\pi_i(x)}, deg(\overline{\pi_i}) = [\mathbb{F}_p(\zeta_q) : \mathbb{F}_p] = \ell =$ degree of minimal polynomial of ζ_q over $\mathbb{F}_p$.

By the Chinese Remainder Theorem, $\mathbb{F}_p[x]/(\overline{\Phi_q(x)}) \cong \prod_{1 \le i \le k} \mathbb{F}_p[x]/(\overline{\pi_i(x)})$. Each field $\mathbb{F}_p[x]/(\overline{\pi_i(x)})$ has dimension $deg(\overline{\pi}_i) = \ell$ over $\mathbb{F}_p$. $|\mathbb{F}_p[x]/(\overline{\pi_i(x)})| = p^\ell$. By Project 11, any two finite fields of the same cardinality are isomorphic. Hence $\mathbb{F}_p[x]/(\overline{\pi_i(x)}) \cong \mathbb{F}_{p^\ell}$.

Therefore, $\mathbb{F}_p[x]/(\overline{\Phi_q(x)}) \cong \prod_{1\le i\le k} \mathbb{F}_p[x]/(\overline{\pi_i(x)}) = \prod_{1\le i\le k} \mathbb{F}_{p^\ell} = (\mathbb{F}_{p^\ell})^k$. $\mathbb{Z}[\zeta_q]/(p)$ has cardinality p^{q-1} and $(\mathbb{F}_{p^\ell})^k$ has cardinality $p^{\ell k}$, and therefore $p^{\ell k} = p^{q-1}$ and $\ell k = q-1$ as desired.

□

(3) Let $G \subseteq \Gamma_q$. Prove that $(\mathbb{Z}[\zeta_q]/(p))^G$, the fixed ring, is of dimension $[\Gamma_q : G]$ over $\mathbb{F}_p$.

Proof. $\mathbb{Z}[\zeta_q] \cong \mathbb{Z}[x]/(\Phi_q(x))$, where $\Phi_q(x) = x^{q-1}+...+x+1$, is the splitting field of $\Phi_q(x)$ over $\mathbb{Z}$. We would like to find a basis for $\mathbb{Z}[\zeta_q]$. By Vieta's formulas, we have the following property of the roots of $\Phi_q(x)$: $\sum_{1\le i\le q-1} \zeta_q^i = -1$, where $1 = \zeta_q^q$. Hence, we only need $q-1$ roots of unity to define a basis. Choose $\{\zeta_q^i \mid 1 \le i \le q-1\}$ as a basis for $\mathbb{Z}[\zeta_q]$.

$\Gamma_q = \mathrm{Aut}(\mathbb{Q}[\zeta_q])$ acts on $\mathbb{Z}[\zeta_q] = \{a_1\zeta_q + \cdots + a_{q-1}\zeta_q^{q-1} \mid a_i \in \mathbb{Z}\}$ by sending ζ_q to $\zeta_q^m, (m,q) = 1$. $G \subseteq \Gamma_q$ acts on $\mathbb{Z}[\zeta_q]$ in a similar fashion. The ideal $(p) \subseteq \mathbb{Z}[\zeta_q]$ is the additive subgroup of $\mathbb{Z}[\zeta_q]$ that contains all elements in $\mathbb{Z}[\zeta_q]$ which are multiples of p. In other words, for any element $a_1\zeta_q + \cdots + a_{q-1}\zeta_q^{q-1} \in (p)$, $a_i \mid p$. Any permutation of the basis of $\mathbb{Z}[\zeta_q]$ leaves the coefficients a_i untouched. Therefore, $G(p) = (p)$. Now we can conclude that G also acts on $\mathbb{Z}[\zeta_q]/(p)$.

Act with G on $\mathbb{Z}[\zeta_q]/(p)$. $dim_{\mathbb{F}_p}(\mathbb{Z}[\zeta_q]/(p))^G = |(\mathbb{Z}[\zeta_q]/(p))/G|$ and $|(\mathbb{Z}[\zeta_q]/(p))/G| = \frac{1}{|G|}\sum_{g\in G} |\mathbb{Z}[\zeta_q]/(p)^g|$ by Burnside's lemma. At the same time, $\sum_{g\in G} |\mathbb{Z}[\zeta_q]/(p)^g| = |\Gamma_q|$. Therefore, $dim_{\mathbb{F}_p}(\mathbb{Z}[\zeta_q]/(p))^G = \frac{|\Gamma_q|}{|G|}$. But $\frac{|\Gamma_q|}{|G|} = [\Gamma_q : G]$ by the orbit-stabilizer theorem. Hence, $dim_{\mathbb{F}_p}(\mathbb{Z}[\zeta_q]/(p))^G = [\Gamma_q : G]$.

□

(4) Prove that ℓ is the least number such that $q \mid p^\ell - 1$. (Note that this is consistent with the fact that $p^{q-1} \equiv 1 \pmod q$)

Proof. First we will show that ℓ satisfies $q \mid p^\ell - 1$, and then we will show that ℓ is the least number for which this condition holds.

From part 2 we know that $\overline{\Phi_q(x)}$ factors over $\mathbb{F}_p[x]$ into $\overline{\Phi_q(x)} = \prod_{1\le i\le k} \overline{\pi_i(x)}$ with $deg(\overline{\pi}_i) = \ell$, and $\mathbb{Z}[\zeta_q]/(p) \cong \mathbb{F}_p[x]/(\overline{\Phi_q(x)}) \cong \prod_{1\le i\le k} \mathbb{F}_p[x]/(\overline{\pi_i(x)})$, where each $\overline{\pi_i}$ has splitting field $\mathbb{F}_{p^\ell}$ over $\mathbb{F}_p$. Each $\overline{\pi}_i$ has ℓ roots over its splitting field and each root is a primitive q-th root of unity. Then, by Project 12, since $\mathbb{F}_{p^\ell}$ contains a primitive q-th root of unity, it contains all q-th roots of unity. Hence, the q-th roots of unity form a subgroup of the multiplicative group of $\mathbb{F}_{p^\ell}$,

$\langle \zeta_q \rangle \subseteq (\mathbb{F}_{p^\ell})^\times$. By Lagrange's Theorem, $|\langle \zeta_q \rangle| \mid |(\mathbb{F}_{p^\ell})^\times|$. But $|\langle \zeta_q \rangle| = |\zeta_q| = q$ and $|(\mathbb{F}_{p^\ell})^\times| = |\mathbb{F}_{p^\ell}| - 1 = p^\ell - 1$. Thus, $q \mid p^\ell - 1$.

Now we will show that ℓ is the least number such that $q \mid p^\ell - 1$. By part 2, $\mathbb{F}_{p^\ell}$ is the splitting field of $\overline{\pi}_i$ over $\mathbb{F}_p$ and $[\mathbb{F}_{p^\ell} : \mathbb{F}_p] = deg(\overline{\pi}_i) = \ell$. By definition, $\mathbb{F}_{p^\ell}$ is the smallest field extension over which $\overline{\pi}_i$ splits. Consequently, ℓ is the minimum number such that the division condition holds.

□

CHAPTER 22

ζ_p and $\sqrt{(-1)^{(p-1)/2}}$

by Jonathan Roth

THEOREM. *q is a prime number.*

(1) *Let R be an integral domain totally ramified at a prime p over $\mathbb{Z}$. Suppose $S \subseteq R$ with $S \neq \mathbb{Z}$, and suppose $\operatorname{pTor} R/S =_{\text{def}} \{r \in R/S | pr = 0\}$ is trivial. Then S is ramified at p.*
(2) *If G is a subgroup of Γ_q then $\mathbb{Z}[\zeta_q]^G$ is totally ramified at q and at no other primes.*
(3) *Let q be odd and G be the unique subgroup of Γ_q of index 2. Then $\mathbb{Z}[\zeta_q]^G$ is a subring of $\mathcal{O}_{(-1)^{(q-1)/2}q}$ and $[\mathcal{O}_{(-1)^{(q-1)/2}q} : \mathbb{Z}[\zeta_q]^G]$ is a power of q.*

PROOF. (1) We consider the natural map from S/pS into R/pR given by

$$\begin{aligned} \varphi : & S/pS \to R/pR \\ & \bar{x} \mapsto \bar{x} \end{aligned}$$

We note that φ is well-defined, since if $x \equiv y \mod pS$, then $x = y + ps$ for some $s \in S \subseteq R$, and hence $x \equiv y \mod pR$ as well. Moreover, it is obvious that φ is a homomorphism.

Now, observe that $\ker(\varphi) = \{\bar{s} \in S/pS | \exists r \in R \text{ s.t. } s = pr\}$.

However, we can also construct the map

$$\begin{aligned} \psi : & \operatorname{pTor}(R/S) \to S/pS \\ & \bar{r} \mapsto \bar{pr} \end{aligned}$$

Then, by construction of $\operatorname{pTor}(R/S)$ and ψ, we have that $\operatorname{im}\psi = \{\bar{s} \in S/pS | \exists r \in R \text{ s.t. } s = pr\} = \ker(\varphi)$. And since by assumption $\operatorname{pTor} R/S = 0$, we have that $\ker(\varphi) = 0$, and hence that φ is injective.

Thus, $S/pS \simeq \operatorname{im}\varphi$. By definition of total ramification, we have that $R/pR \simeq \mathbb{F}_p[t]/(t^d)$, where $d = \dim_{\mathbb{Q}} R \otimes_{\mathbb{Z}} \mathbb{Q}$, and so S/pS is isomorphic to a subring of $\mathbb{F}_p[t]/(t^d)$. Then to show that S is ramified at p, it suffices to show that $S/pS \neq \mathbb{Z}/pZ$. Indeed, if this is the case, then S/pS contains an element of the form $c_{d-1}t^{d-1} + \ldots + c_1 t + c_0$, where $c_i \in \mathbb{F}_p$ for all i, and $c_i \neq 0$ for some $i > 0$. But $\mathbb{Z} \subset S$, and so $\mathbb{F}_p \subseteq S/pS$. Thus, since S/pS is a subring, it also contains

$c_{d-1}t^{d-1} + \ldots + c_1 t$. By construction this element is non-zero, but equals zero when raised to the d-th power, so S is ramified at p.

However, from Problem 14, since S is finitely generated as an abelian group, we have that there exists a natural number k, primes $p_1, \ldots, p_n$, and for each p_i natural numbers $e_{j1}, \ldots, e_{j\ell_i}$ and $r_{j1}, \ldots, r_{j\ell_i}$ such that

$$S \simeq \mathbb{Z}^k \oplus \prod_{i=1}^{k} \prod_{j=1}^{\ell_i} (\mathbb{Z}/p^{e_{ji}})^{r_{ji}}$$

However, R is an integral domain, and so $S \subseteq R$ is an integral domain and hence torsion free. It thus must be that the terms to the right of the product above are 0, so that $S \simeq \mathbb{Z}^k$. Moreover, since $S \neq \mathbb{Z}$, we have that $k \neq 1$. Hence, $S/pS \simeq (\mathbb{Z}/p\mathbb{Z})^k \neq \mathbb{Z}/pZ$, as needed.

(2) First, observe that $\mathbb{Z}[\zeta_q]$ is finitely generated as an abelian group, and hence $\mathbb{Z}[\zeta_q]^G \subseteq \mathbb{Z}[\zeta_q]$ is finitely generated as an abelian group. Therefore, by Problem 14, there exists a natural number k, primes $p_1, \ldots, p_n$, and for each p_i natural numbers $e_{j1}, \ldots, e_{j\ell_i}$ and $r_{j1}, \ldots, r_{j\ell_i}$ such that as an additive group

$$\mathbb{Z}[\zeta_q]^G \simeq \mathbb{Z}^k \oplus \prod_{i=1}^{k} \prod_{j=1}^{\ell_i} (\mathbb{Z}/p^{e_{ji}})^{r_{ji}}$$

However, $\mathbb{Z}[\zeta_q]^G \subseteq \mathbb{Z}[\zeta_q] \subseteq \mathbb{Q}(\zeta_q)$ as an additive subgroup, and since $\mathbb{Q}(\zeta_q)$ is torsion-free, it must be that $\mathbb{Z}[\zeta_q]^G$ is torsion-free as well. Therefore, as before, the terms to the right of the product must be 0, so that $\mathbb{Z}[\zeta_q]^G \simeq \mathbb{Z}^k$ as an additive group.

Now, observe that if $x \in \mathbb{Q}[\zeta_q]^G$, then there exists $n \in \mathbb{Z}$ such that $nx \in \mathbb{Z}[\zeta_q]^G$. Indeed, n can be taken to be the product of the denominators of the coefficients on $1, \zeta_q, \ldots \zeta_q^{q-1}$. Hence, we have that $\mathbb{Z}[\zeta_q]^G \otimes \mathbb{Q} \simeq \mathbb{Q}[\zeta_q]^G$. Now, let $d = [\Gamma_q : G]$. Then by the Galois correspondence, $\dim_{\mathbb{Q}} \mathbb{Q}[\zeta_q]^G = d$, so $\dim_{\mathbb{Q}} \mathbb{Z}[\zeta_q]^G \otimes \mathbb{Q} = d$. Thus, we have $\mathbb{Z}[\zeta_q]^G \otimes \mathbb{Q} \simeq \mathbb{Q}[\zeta_q]^G \simeq \mathbb{Q}^d$. But then $\mathbb{Z}[\zeta_q]^G \otimes \mathbb{Q} \simeq \mathbb{Z}^k \otimes \mathbb{Q} \simeq (\mathbb{Z} \otimes \mathbb{Q})^k \simeq \mathbb{Q}^k$, so it must be that $k = d$.

Hence, $\mathbb{Z}[\zeta_q]^G \simeq \mathbb{Z}^d$, so as an additive group, $\mathbb{Z}[\zeta_q]^G/(q) \simeq \mathbb{Z}^d/(q) \simeq (\mathbb{Z}/(q))^d \simeq \mathbb{F}_q[t]/(t^d)$, where $d = \dim_{\mathbb{Q}} \mathbb{Z}[\zeta_q]^G \otimes \mathbb{Q}$.

It remains to show that $\mathbb{Z}[\zeta_q]^G/(q) \simeq \mathbb{F}_q[t]/(t^d)$ as a multiplicative group as well. To do this, let α be a generator of $\mathbb{F}_q^\times$, and recall that $d = [\Gamma_q : G]$, so that $|G| = \frac{q-1}{d}$. For any element $k \in \mathbb{F}_q^\times$, denote by γ_k the automorphism $\zeta_q \mapsto \zeta_q^{\alpha^k}$. We claim that γ_d generates G. To see this, first observe that for any $a, b \in \mathbb{F}_q^\times$, $\gamma_a \circ \gamma_b = \gamma_{a+b}$, since $(\zeta_q^{\alpha^a})^{\alpha^b} = \zeta_q^{\alpha^{a+b}}$. In addition, α generates $\mathbb{F}_q^\times$, so $\alpha^{kd} \equiv 1 \mod q$ for $k = \frac{q-1}{d}$, but not for any lesser k. Hence, $(\gamma_d) = \{1, (\gamma_d), (\gamma_d)^2, \ldots, (\gamma_d)^{\frac{q-2}{d}}\} = \{1, \gamma_d, \gamma_{2d}, \ldots, \gamma_{q-2}\}$, which is cyclic of order $\frac{q-1}{d}$.

But by Project 13, Γ_q is cyclic, and hence Γ_q has only one subgroup of order $\frac{q-1}{d}$. Thus, we must have $(\gamma_d) = G$.

Now, we consider the orbit of the element ζ_q^α. From the above characterization of G, we have that $\text{Orb}(\zeta_q^\alpha) = \{\zeta_q^\alpha, \zeta_q^{\alpha^{1+d}}, \zeta_q^{\alpha^{1+2d}} \dots \zeta_q^{\alpha^{1+(q-2)}}\}$. It follows directly that $\eta =_{\text{def}} \prod_{k=0}^{(q-2)/d}(1 - \zeta^{\alpha^{1+dk}})$ is fixed by G , and hence $\eta \in \mathbb{Z}[\zeta_q]^G$.

We claim that $\bar{\eta}$ generates $\mathbb{Z}[\zeta_q]^G/(p)$. In order to show this, we first derive a number of results relating to the elements of the form $(1 - \zeta^i)$.

RESULT 1. $\prod_{i=1}^{q-1}(1 - \zeta^i) = q$

PROOF. By construction of ζ, we have that

$$\prod_{i=0}^{q-1}(t - \zeta^i) = t^q - 1$$

Factoring out $(t - 1)$ from both sides, it follows that

$$\prod_{i=1}^{q-1}(t - \zeta^i) = t^{q-1} + t^{q-2} + \ldots + 1$$

Evaluating at $t = 1$ gives

$$\prod_{i=1}^{q-1}(1 - \zeta^i) = 1^{q-1} + 1^{q-2} + \ldots + 1 = q,$$

as needed.

□

RESULT 2. *If n is a natural number and x and y are in a ring R, then $x^n - y^n$ is divisible by $x - y$.*

PROOF. The statement is trivially true for $n = 1$. Suppose the statement holds for $n = 1, \ldots, k$.

Then

$$\begin{aligned} x^{k+1} - y^{k+1} &= x^{k+1} - xy^k + xy^k - y^{k+1} \\ &= x(x^k - y^k) + (x - y)y^k \end{aligned}$$

Clearly, the second term is divisible by $x-y$. And by the inductive hypothesis, the first term is divisible by $x - y$ as well, so $x^{k+1} - y^{k+1}$ is divisible by $x - y$. □

RESULT 3. *For any $i, j \in \{1, \ldots, q-1\}$, $(1 - \zeta^i) = c(1 - \zeta^j)$, where c is a unit*

PROOF. It suffices to show that for any $i \in \{1, \ldots, q-1\}$, there exists a unit c such that $(1-\zeta^i) = c(1-\zeta)$. To do this, observe that $1-\zeta^i = 1^i-\zeta^i$, so by Result 2, $(1 - \zeta^i) = c(1 - \zeta)$, for some c. However, there exists some k for which $ik \equiv 1 \mod q$, and hence $1 - \zeta = 1^k - (\zeta^i)^k$. Thus, by Result 2, $(1 - \zeta) = c'(1 - \zeta^i)$. It then follows that $c'c = 1$, so that c is a unit as needed. □

RESULT 4. *For any $d_1, \ldots, d_{q-1} \in \{1, \ldots, q-1\}$, $\prod_{i=1}^{q-1}(1-\zeta^{d_i}) = cq$, where c is a unit.*

PROOF. From the previous result $(1-\zeta^{d_i}) = c_i(1-\zeta^i)$, where c_i is a unit. Thus,

$$\begin{aligned}\prod_{i=1}^{q-1}(1-\zeta^{d_i}) &= \prod_{i=1}^{q-1} c_i(1-\zeta^i) \\ &= \left(\prod_{i=1}^{q-1} c_i\right)\left(\prod_{i=1}^{q-1}(1-\zeta^i)\right) \\ &= cq\end{aligned}$$

where $c =_{\text{def}} \prod_{i=1}^{q-1} c_i$, which is clearly a unit since the c_i are units. □

RESULT 5. *For any $i \in \{1, \ldots, q-1\}$, $1-\zeta^i$ is not a unit.*

PROOF. It suffices to show that this holds for $1-\zeta$, since for any i, $(1-\zeta^i)$ is merely a unit multiple of $(1-\zeta)$. Suppose for contradiction that there exists $x \in \mathbb{Z}[\zeta_q]$ such that $(1-\zeta)x = 1$. Then $x = c_0 + c_1\zeta + \ldots c_{q-1}\zeta^{q-1}$ for some $c_0, \ldots, c_{q-1} \in \mathbb{Z}$. We have

$$\begin{aligned}&(1-\zeta)(c_0 + c_1\zeta + \ldots + c_{q-1}\zeta^{q-1}) = \\ &\quad c_0 + c_1\zeta + \ldots + c_{q-1}\zeta^{q-1} - \\ &\quad c_{q-1} + c_0\zeta + \cdots + c_{q-2}\zeta^{q-1} = \\ &\quad (c_0 - c_{q-1}) + (c_1 - c_2)\zeta + \ldots + (c_{q-1} - c_{q-2})\zeta^{q-1} = \\ &\quad 1\end{aligned}$$

It follows that

$$\begin{cases} 1 = c_0 - c_{q-1} \\ 0 = c_1 - c_2 = \ldots = c_{q-1} - c_{q-2} \end{cases}$$

However, the second equation implies that $c_0 = \ldots = c_{q-1}$, which contradicts the first equation. Therefore, it must be that no such x exists, so that $1-\zeta$ is a non-unit. □

RESULT 6. *Let I be a collection of $q-1$ elements of $\{1, \ldots, q-1\}$. Let H be a strict subcollection of I. Then $\prod_{h\in H}(1-\zeta^h)$ is not a multiple of q in $\mathbb{Z}[\zeta_q]$.*

PROOF. By Result 4, we have that for some unit c,

$$\prod_{i\in I}(1-\zeta^i) = cq \tag{59}$$

$$\implies c^{-1}\prod_{i\in I}(1-\zeta^i) = q \tag{60}$$

Suppose, for contradiction, that

$$\prod_{h\in H}(1-\zeta^h) = pq \tag{61}$$

where $p \in \mathbb{Z}[\zeta_q]$ is not necessarily a unit.

Let $\mu = \prod_{i\notin H}(1-\zeta^i)$. Then using Equations 60 and 61, we have

$$c^{-1}\left(\prod_{i\notin H}(1-\zeta^i)\right)\left(\prod_{h\in H}(1-\zeta^h)\right) = q \tag{62}$$

$$\implies c^{-1}\cdot\mu\cdot pq = q \tag{63}$$

$$\implies \mu\cdot(c^{-1}p)q = q \tag{64}$$

$$\implies \mu(c^{-1}p) = 1. \tag{65}$$

This implies that $\mu = \prod_{i\notin H}(1-\zeta^i)$ is a unit. However, from Result 5, we know that $(1-\zeta^i)$ is a not a unit for all i, and hence the product of such terms cannot be a unit as well. Contradiction. It must be that Equation 61 cannot hold for any p. □

Now, η is the product of $\frac{q-1}{d}$ terms of the form $(1-\zeta^i)$. Hence, η^d is the product of $q-1$ terms of this form, and thus η^d is a multiple of q by Result 4. However, by Result 6, q does not divide η^k for $k = 1,\dots,d-1$. It follows that $\bar{\eta}$ generates a subgroup of $\mathbb{Z}[\zeta_q]^G/(q)$ of order q^d. But as an additive group, $\mathbb{Z}[\zeta_q]^G/(q) \simeq \mathbb{F}_q[t]/(t^d)$, so it has precisely q^d elements. Thus, $\bar{\eta}$ generates $\mathbb{Z}[\zeta_q]^G/(q)$ as a multiplicative group. It is then clear that the map sending $\bar{\eta}$ to $\bar{t}$ is an isomorphism, so that $\mathbb{Z}[\zeta_q]^G/(q) \simeq \mathbb{F}_q[t]/(t^d)$ as a multiplicative group as well.

Thus $\mathbb{Z}[\zeta_q]^G$ is totally ramified at q.

Now, let $p \neq q$ be prime. Suppose that $\mathbb{Z}[\zeta_q]^G$ is totally ramified at p. Then by definition, $\mathbb{Z}[\zeta_q]^G \simeq \mathbb{F}_p[t]/(t^d)$, where $d = \dim_{\mathbb{Q}} \mathbb{Z}[\zeta_q]^G \otimes \mathbb{Q}$. The element identified with $\bar{t}$ is then nilpotent, so $\mathbb{Z}[\zeta_q]^G$ is ramified at p. But $\mathbb{Z}[\zeta_q]^G \subseteq \mathbb{Z}[\zeta_q]$, and so this implies that $\mathbb{Z}[\zeta_q]$ is ramified at p as well. However, since p and q are distinct primes, by Problem 16.3, we have that $\mathbb{Z}[\zeta_q]$ is unramified at p. Contradiction. It must be that $\mathbb{Z}[\zeta_q]^G$ is not totally ramified at p.

(3) Observe that since $[\Gamma_q : G] = 2$, we have that $\dim_{\mathbb{Q}} \mathbb{Q}[\zeta_q]^G = 2$. Now, let $\alpha \in \mathbb{Q}[\zeta_q]^G$ such that $\alpha \notin \mathbb{Q}$. Then $\{1,\alpha\}$ forms a basis of $\mathbb{Q}[\zeta_q]^G$, and so $\mathbb{Q}[\zeta_q]^G = \mathbb{Q}(\alpha)$. In addition, since $\mathbb{Q}[\zeta_q]^G$ is of degree 2, we have that $\{1,\alpha,\alpha^2\}$ is linearly dependent. Hence, there is a polynomial $f(x) = x^2+bx+c$, with $b,c \in \mathbb{Q}$, such that $f(\alpha) = 0$. But then by the quadratic formula, $\alpha = -b/2 \pm \sqrt{b^2/4-c} = -b/2 \pm \sqrt{\Delta}$, where $\Delta = b^2/4 - c$. And Δ must be square-free, since otherwise we would have that $\alpha \in \mathbb{Q}$. Thus, since α generates $\mathbb{Q}[\zeta_q]^G$ and α and $\sqrt{\Delta}$ differ only

by a constant in $\mathbb{Q}$, we have that $\mathbb{Q}[\zeta_q]^G = \mathbb{Q}(\Delta)$.

Hence, $\mathbb{Z}[\zeta_q]^G \subseteq \mathbb{Q}[\zeta_q]^G = \mathbb{Q}(\sqrt{\Delta})$. However, we know that every element of $\mathbb{Z}[\zeta_q]^G$ is an algebraic integer, and hence that $\mathbb{Z}[\zeta_q]^G \subseteq \mathcal{O}_\Delta$.

Now, let p be a prime not equal to q. We consider the reduction map

$$\begin{aligned}\rho :&\mathbb{Z}[\zeta_q]^G/(p) \to (\mathbb{Z}[\zeta_q]/(p))^G\\ &\bar{x} \mapsto \bar{x}\end{aligned}$$

It should be clear that this map is well-defined, since if $x \in \mathbb{Z}[\zeta_q]$ is fixed by G, then x must also be fixed by G when first modding out by p; that is if $x \in \mathbb{Z}[\zeta_q]^G$, then $gx = x$ for all $g \in G$, and so $g\bar{x} = \bar{gx} = \bar{x}$. In addition, ρ is obviously a homomorphism.

Moreover, it can be shown that ρ is injective.[1] It follows that $\mathbb{Z}[\zeta_q]^G/(p)$ is isomorphic to the image of ρ in $(\mathbb{Z}[\zeta_q]/(p))^G$. However, since p and q are distinct primes, from Problem 16 we know that p is unramified in $\mathbb{Z}[\zeta_q]$. Thus, there are no nilpotent elements in $\mathbb{Z}[\zeta_q]/(p)$, and so it follows there are no nilpotents elements in any subgroups of $\mathbb{Z}[\zeta_q]/(p)$. We showed earlier, however, that $\mathbb{Z}[\zeta_q]^G/(p) \simeq \operatorname{im}\rho \subseteq (\mathbb{Z}[\zeta_q]/(p))^G \subseteq \mathbb{Z}[\zeta_q]/(p)$. Hence, $\mathbb{Z}[\zeta_q]^G/(p)$ has no nilpotent elements, and so $\mathbb{Z}[\zeta_q]^G$ is not ramified at p.

We have thus shown that $\mathbb{Z}[\zeta_q]^G$ is ramified at most at q. But we showed earlier that $\mathbb{Z}[\zeta_q]^G \subseteq \mathcal{O}_\Delta$, where Δ is square-free. From Problem 20.4, we have that if p ramifies in $\mathcal{O}_\Delta$, then p ramifies in any subring, and so it follows that $\mathcal{O}_\Delta$ ramifies at most at q. Then applying the result of Problem 20.3, we have that $\Delta = (-1)^{(q-1)/2}$, as needed.

In addition, from Problem 20.4, we have that if a prime p divides $\#\mathcal{O}_\Delta/\mathbb{Z}[\zeta_q]^G$, then p ramifies in $\mathbb{Z}[\zeta_q]^G$. But $\mathbb{Z}[\zeta_q]^G$ ramifies at no primes other than q, and so it must be that the only prime that divides $\#\mathcal{O}_\Delta/\mathbb{Z}[\zeta_q]^G$ is q. Thus, $[\mathcal{O}_\Delta : \mathbb{Z}[\zeta_q]^G] = \#\mathcal{O}_\Delta/\mathbb{Z}[\zeta_q]^G$ is a power of q.

□

[1] Professor Silberstein said that this can be assumed for the purposes of this proof

CHAPTER 23

Pulling it All Together

by Charles Jeon

Let G be as in the last section.

PROBLEM 1. Prove that a prime $p \neq q$ splits in $\mathbb{Z}[\zeta_q]^G$ if and only if $\left(\frac{p}{q}\right) = 1$.

PROOF. Note that in Problem 13, we have defined $\Gamma_q = \mathrm{Aut}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) = (\mathbb{Z}/q\mathbb{Z})^\times$ which sends the automorphism ϕ_l given by $\phi_l(\zeta_q) = \zeta_q^l$ for $l \in (\mathbb{Z}/q\mathbb{Z})^\times$. This is inductive because the reduction from $\mathbb{Z} \to \mathbb{Z}/q\mathbb{Z}$ is injective on the q-th root of unity ζ_q. We also know from Problem 21 that Γ_q is cyclic of order $q-1$ and G is the unique subgroup of Γ_q of index 2 by Problem 22. Let us consider G to be square elements of Γ_q. Then, we know that the image of G in $(\mathbb{Z}/q\mathbb{Z})^\times$ is composed of all the multiplicative quadratic residues $\bmod q$. If we now consider a prime $p \neq q$, we note that G takes the square root of q in $(\mathbb{Z}/q\mathbb{Z})^\times$. For this to be true, $p \equiv n^2 \mod q$ for some $n \in \mathbb{Z}$, so we have that $\left(\frac{p}{q}\right) = 1$ for ϕ_p to be in G. □

PROBLEM 2. Prove that a prime $p \neq q$ splits in $\mathbb{Z}[\zeta_q]^G$ if and only if p splits in $\mathcal{O}_{(-1)^{(q-1)/2}q}$.

PROOF. Using the results from Problem 22, we are given that $\mathbb{Z}[\zeta_q]^G$ is a subring of $\mathcal{O}_{(-1)^{(q-1)/2}q}$ and $\left[\mathcal{O}_{(-1)^{(q-1)/2}q} : \mathbb{Z}[\zeta_q]^G\right]$ is a power of q. Therefore, if a prime $p \neq q$ splits in $\mathcal{O}_{(-1)^{(q-1)/2}q}$, it has to split $\mathbb{Z}[\zeta_q]^G$. Note that we can also show this using Gauss-sum $\tau = \sum_t \left(\frac{t}{q}\right)\zeta^t$ where t ranges over all the non-zero residue classes $\bmod q$. Since $\tau^2 = (-1)^{(q-1)/2}q \in \mathbb{Z}[\zeta_q]^G$, $\mathbb{Z}[\zeta_q]^G = \mathcal{O}_{(-1)^{(q-1)/2}q}$. □

PROBLEM 3. Deduce that $\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}\left(\frac{q}{p}\right)$.

PROOF. From the first problem, we have shown that $p \neq q$ splits in $\mathbb{Z}[\zeta_q]^G$ if and only if $\left(\frac{p}{q}\right) = 1$. Moreover, from the second problem, this happens if and only if p splits in $\mathcal{O}_{(-1)^{(q-1)/2}q}$ which is given as the ring of algebraic integers in $\mathbb{Z}\left(\sqrt{(-1)^{(q-1)/2}q}\right)$ in Problem 5. Using the result of Problem 19, prime $p \neq q$ splits this if and only if $\left(\frac{(-1)^{(q-1)/2}q}{p}\right) = 1$. Now we use this to show the law of **quadratic reciprocity**.

First, suppose that $q \equiv 1 \mod 4$. Then, $(-1)^{(q-1)/2} q = q$, so we have that

$$\left(\frac{(-1)^{(q-1)/2} q}{p} \right) = \left(\frac{q}{p} \right)$$

However, now, suppose that $q \equiv 3 \mod 4$. Then,

$$\left(\frac{(-1)^{(q-1)/2} q}{p} \right) = \left(\frac{-q}{p} \right) = \left(\frac{-1}{p} \right) \left(\frac{q}{p} \right) = \begin{cases} + \left(\frac{q}{p} \right) & \text{if } p \equiv 1 \mod 4 \\ - \left(\frac{q}{p} \right) & \text{if } p \equiv 3 \mod 4 \end{cases}$$

This can be expressed compactly by

$$\therefore \left(\frac{p}{q} \right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \left(\frac{q}{p} \right)$$

Another version of this proof using Gauss sums is shown below. □

REMARK 1. Another version of law of quadratic reciprocity using Gauss sums and showing $\tau_q^2 = (-1)^{(q-1)/2} q$

PROOF. If we denote ζ be a q-th root of unity, let the Gauss Sum τ be defined as

$$\tau_q = \sum_t \left(\frac{t}{q} \right) \zeta^t$$

where t ranges over all the non-zero residue classes $\mod q$. Before proceeding with the proof, let us show that $\tau_q^2 = (-1)^{\frac{q-1}{2}} q$. Starting with

$$\tau_q^2 = \sum_r \sum_s \left(\frac{rs}{q} \right) \zeta^{r+s}$$

we note that for a fixed s, the product rs goes all the non-zero residue classes (q is prime). Therefore, if we replace r as rs,

$$\begin{aligned} \tau_q^2 &= \sum_{r,s} \left(\frac{rs^2}{q} \right) \zeta^{rs+s} = \sum_{r,s} \left(\frac{r}{q} \right) \zeta^{s(r+1)} \\ &= \sum_s \left(\frac{-1}{q} \right) \zeta^0 + \sum_{r \neq q-1, s} \left(\frac{r}{q} \right) \zeta^{s(r+1)} \\ &= (q-1) \left(\frac{-1}{q} \right) + \sum_{r \neq q-1} \left(\frac{r}{q} \right) \sum_s \zeta^{s(r+1)} \end{aligned}$$

However, for $r \neq -1$, we have that

$$\sum_s \zeta^{s(r+1)} = \zeta^{r+1} + \zeta^{2(r+1)} + \cdots + \zeta^{(q-1)(r+1)}$$

We note that this has to equal -1 because $\zeta^{r+1} \neq 1$ and $1 + \zeta^{r+1} + \cdots + \zeta^{(q-1)(r+1)} = 0$. Thus, τ^2 now becomes

$$\begin{aligned} \tau_q^2 &= (q-1)\left(\frac{-1}{q}\right) - \sum_{r \neq q-1}\left(\frac{r}{q}\right) = q\left(\frac{-1}{q}\right) - \sum_r \left(\frac{r}{q}\right) \\ &= q\left(\frac{-1}{q}\right) \end{aligned}$$

because there are equal number of $+1$ and -1 in the $\sum_r \left(\frac{r}{q}\right)$. Now, let us proceed back to the problem by considering $\tau_q^p \mod p$ and the properties found in previous sections

$$\begin{aligned} \tau_q^p &\equiv \tau_q \left(\tau_q^2\right)^{\frac{p-1}{2}} \equiv \tau_q \left(q\left(\frac{-1}{q}\right)\right)^{\frac{p-1}{2}} \\ &\equiv \tau_q q^{\frac{p-1}{2}} (-1)^{\frac{q-1}{2}\frac{p-1}{2}} \\ &\equiv \tau_q \left(\frac{q}{p}\right)(-1)^{\frac{q-1}{2}\frac{p-1}{2}} \end{aligned}$$

If we evaluate τ_q^p directly, we obtain

$$\begin{aligned} \tau_q^p &\equiv \left(\sum_t \left(\frac{t}{q}\right)\zeta^t\right)^p \equiv \sum_t \left(\frac{t}{q}\right)^p \zeta^{tp} \\ &\equiv \left(\frac{p}{q}\right)^2 \sum_t \left(\frac{t}{q}\right)\zeta^{tp} \\ &\equiv \left(\frac{p}{q}\right)\sum_t \left(\frac{tp}{q}\right)\zeta^{tp} \\ &\equiv \left(\frac{p}{q}\right)\tau_q \end{aligned}$$

because p is both odd and prime. Using the two results, we have

$$\tau_q \left(\frac{q}{p}\right)(-1)^{\frac{q-1}{2}\frac{p-1}{2}} \equiv \left(\frac{p}{q}\right)\tau_q$$

which leads us to

$$\tau_q^2 \left(\frac{q}{p}\right)(-1)^{\frac{q-1}{2}\frac{p-1}{2}} \equiv \left(\frac{p}{q}\right)\tau_q^2$$

However, $\tau_q^2 = \pm q$ which is coprime to p (assumption), so we are left with

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right)$$

□