Number Theory Notes

JH

Date

Contents

Chapter 1

Finite Fields

1.1 Generalities

1.1.1 Finite fields

Definition – Characteristic of a field
If K is a field then the map $\mathbb{Z} \to K$ induced by $1 \mapsto 1$ is a ring morphism. The image of this morphism is an integral domain since K is a field, hence the kernel is a prime ideal. Since $\mathbb{Z}$ is a PID, we can define the characteristic of K, denoted $\mathrm{Char}(K)$ to be the positive generator of the kernel.

Proposition – Frobenius map
If K is a field and $\mathrm{Char}(K)$ is prime then

$$\sigma_p : K \to K \quad := \quad x \mapsto x^p$$

is an injection.

Proof. Easy to show $\sigma_p(0) = 0, \Sigma_p(1) = 1$. Also

$$\sigma_p(ab) = (ab)^p = a^p b^p = \sigma_p(a)\sigma_p(b)$$
$$\sigma_p(a + b) = (a + b)^p = a^p + b^p = \sigma(a) + \sigma(b)$$

by expanding the binomial and noting that when $1 \leq k \leq p$, $p \mid \binom{p}{k} k!(p-k)!$ and is coprime to the latter two, thus $p \mid \binom{p}{k}$. Since σ_p is a morphism of fields it is injective. □

Proposition – Classification of finite fields
Let K be a finite field and suppose $\Omega \models \mathrm{ACF_p}$ where p is prime and q is a non-trivial power of p. Then

1. $\mathrm{Char}(K) \neq 0$ and $|K| = p^{[K:\mathbb{F}_p]}$

2. $\mathbb{F}_q := \{x \in \Omega \,|\, x^q = x\}$ is the unique subfield of Ω with q elements.
3. If $|K| = q$ then $K \cong \mathbb{F}_q$.

Proof.

1. If $\mathrm{Char}(K) = 0$ then $\mathbb{Z}$ injects into K thus thus $\aleph_0 \leq |\mathbb{Z}| \leq |K|$ which is false. Since $[K : \mathbb{F}_p]$ is the cardinality of any basis B of K as a vector space over $\mathbb{F}_p$ and $K \cong {\mathbb{F}_p}^B$, $|K| = \left|{\mathbb{F}_p}^B\right| = p^{[K:\mathbb{F}_p]}$.
2. Easy to show elementarily that $\mathbb{F}_q$ is a subfield. As polynomials over a field are seperable if and only the gcd of the derivative and the polynomial is 1,
$$D(X^q - X) = qX^{q-1} - 1 = -1$$
Hence it has q distinct roots in the algebraic closure of Ω, namely Ω itself. Hence $|\mathbb{F}_q| = q$. Uniqueness: if $L \leq \Omega$ and $|L| = q$ then for any unit $x \in L \setminus \{0\}$, $x^{q-1} = 1$ by Lagrange and so $x \in \mathbb{F}_q$. Thus $L \subseteq \mathbb{F}_q$ and they have equal finite cardinality, so $L = \mathbb{F}_q$.
3. If L is a field such that $|L| = q$ then the image of $\mathbb{Z}$ in L has cardinality dividing q by Lagrange. Hence $\mathrm{Char}(L) = p$ and the image of $\mathbb{Z}$ is $\mathbb{F}_p$. Finitely generate L over $\mathbb{F}_p$ and for each generator a the minimal polynomial of a over $\mathbb{F}_p$ splits in Ω since it is aglebraically closed. By 'embedding finite extensions via conjugates' in Galois Theory, there is a map $L \to F_q$ which is injective. It is an isomorphism since they have the same finite cardinality.

$\square$

1.1.2 Multiplicative group of a finite field

Definition – Euler's Totient Function
If $1 \leq a \leq d$ in $\mathbb{Z}$ then a is coprime to d if and only if $\overline{a} \in \mathbb{Z}/d\mathbb{Z}$ is a generator since

$$\begin{aligned} & (a,d) = 1 \\ \Leftrightarrow \quad & \exists \lambda, \mu \in \mathbb{Z}, \lambda a + \mu d = 1 \\ \Leftrightarrow \quad & \exists \lambda \in \mathbb{Z}, \overline{\lambda a} = 1 \\ \Leftrightarrow \quad & \langle \overline{a} \rangle = \mathbb{Z}/d\mathbb{Z} \end{aligned}$$

We define Euler's totient function

$$\phi(d) := |\{a \in \mathbb{Z}/d\mathbb{Z} \,|\, \langle a \rangle = \mathbb{Z}/d\mathbb{Z}\}| = |\{a \in \mathbb{Z} \,|\, 1 \leq a \leq d \,\wedge\, (a,d) = 1\}|$$

NOTATION. *For any cyclic group G, let $\Phi(G) = \{g \in G \,|\, \langle g \rangle = G\}$ be the set of generators.*

Proposition – Partitioning cyclic groups
If $n \in \mathbb{Z}_{>0}$ then $n = \sum_{d|n} \phi(d)$.

Proof. Let $n \in \mathbb{Z}_{>0}$ and let d divide n. Then by some cyclic group theory there exists a unique cyclic subgroup $C_d \leq \mathbb{Z}/n\mathbb{Z}$ with cardinality d. We want to show that $\mathbb{Z}/n\mathbb{Z} = \bigsqcup_{d|n} \Phi(C_d)$. Indeed if $x \in \mathbb{Z}/n\mathbb{Z}$ then $\langle x \rangle$ has some order d dividing n by Lagrange. Hence $x \in \Phi(\langle x \rangle) = \Phi(C_d)$. Thus $\mathbb{Z}/n\mathbb{Z} \subseteq \cup_{d|n} \Phi(C_d)$.

To show it is disjoint notice that if x is in $\Phi(C_d) \cap \Phi(C_e)$ then d and e are both the order of x. □

Proposition – Sufficient condition for cyclic
Let G be a group such that for any $d \mid |G|$,

$$\left|\left\{x \in G \,|\, x^d = e\right\}\right| \leq d$$

then G is cyclic.

Proof. We show that for all divisors of $|G|$ there is an element of G of that order. Then in particular $|G| \mid |G|$ and so there is a generator of G.

Let $d \mid G$. Consider $\{x \in G \,|\, x \text{ has order } d\}$. If it is non-empty, then take such an x:

$$\langle x \rangle \subseteq \left\{g \in G \,|\, g^d = e\right\}$$

and so $d \leq |\langle x \rangle| \leq \left|\left\{g \in G \,|\, g^d = e\right\}\right| \leq d$. Then $\langle x \rangle = \left\{g \in G \,|\, g^d = e\right\}$. Hence for $g \in G$,

$$\begin{aligned} g \text{ has order } d &\Leftrightarrow g \text{ has order } d \wedge g^d = e \\ &\Leftrightarrow g \text{ has order } d \wedge g \in \langle x \rangle \\ &\Leftrightarrow \langle g \rangle = \langle x \rangle \end{aligned}$$

Hence $|\{x \in G \,|\, x \text{ has order } d\}| = \phi(d)$ In either case, (empty or not), $|\{x \in G \,|\, x \text{ has order } d\}| \leq \phi(d)$

Assume for a contradiction that there exists a d such that $\{x \in G \,|\, x \text{ has order } d\}$ is empty. Then partitioning

$$G = \bigsqcup_{d \,\mid\, |G|} \{x \in G \,|\, x \text{ has order } d\}$$

we have that

$$|G| = \sum_{d||G|} |\{x \in G \,|\, x \text{ has order } d\}| < \sum_{d||G|} \phi(d) = |G|$$

a contradiction. □

Proposition – $\mathbb{F}_q^*$ is cyclic
Suppose $d \mid \left|\mathbb{F}_q^*\right|$. Then since $\mathbb{F}_q[X]$ has division algorithm,

$$\left|\left\{x \in \mathbb{F}_q^* \,|\, x^d = 1\right\}\right| \leq d$$

Hence $\mathbb{F}_q^*$ is cyclic.

1.2 Equations over a finite field

Proposition

Power sums lemma Let $u \in \mathbb{N}$ and K be field with $|K| = q$ a power of a non-trivial prime. Then

$$\sum_{x \in K} x^u = \begin{cases} -1 & , 1 \leq u \wedge q-1 \mid u \\ 0 & , \text{otherwise} \end{cases}$$

Proof. Case $u = 0$ then $\sum_{x \in K^n} x^u = \sum_{x \in K^n} 0 = 0$.

Case $1 \leq u \wedge q-1 \mid u$ then for some d,

$$\sum_{x \in K} x^u = \sum_{x \in K} (x^(q-1))^d == \sum_{x \in K^*} 1^d = (q-1)1 = -1$$

Case $1 \leq u \wedge q-1 \not| u$ then there exist $d, r \in \mathbb{N}$ such that $u = (q-1)d + r$ and $0 < r < q-1$. Let y be a generator of K^* (K^* is cyclic). Then suppose for a contradiction that $y^u = 1$, then $q-1 \mid u$ since $q-1$ is the order of y, a contradiction. Multiplying by y is a bijection on the group, hence

$$\sum_{x \in K^n} x^u = \sum_{x \in K^n} (yx)^u = y^u \sum_{x \in K^n} x^u$$

Thus $(1 - y^u) \sum_{x \in K^n} x^u = 0$ and so $\sum_{x \in K^n} x^u = 0$, as $y^u \neq 1$. □

Definition – Vanishing

Suppose for all $I \subseteq K[x1, \ldots, x_n]$ We define the vanishing of I, $V(I) := \{x \in K^n \mid \forall f \in I, f(x) = 0\}$

Proposition – Chevalley

Suppose for all $f \in I \subseteq K[x1, \ldots, x_n]$ (finite),

$$\sum_{f \in I} \deg f < n$$

Then

$$|V(I)| \stackrel{p}{=} 0$$

Proof. Consider $P := \prod_{f \in I}(1 - f^{q-1})$. This is well defined as I is finite. We show that $V(I) = P^{-1}(1)$. Let $x \in K^n$.

$$x \in V(I) \Rightarrow \forall f \in I, f(x) = 0 \Rightarrow f(x)^{q-1} = 0 \Rightarrow P(x) = 1$$

$$x \notin V \Rightarrow \exists f \in I, f \neq 0 \Rightarrow f(x)^{q-1} = 1 \Rightarrow P(x) = 0$$

Let $S : K[x_1, \ldots, x_n] \to K := f \to \sum_{x \in K^n} f(x)$ Then $S(P) = \sum_{x \in V(I)} 1 \stackrel{p}{=} |V(I)|$. Thus we need show that $S(P) = 0$.

$$\deg P = \sum_{f\in I}(q-1)\deg f = (q-1)\sum_{f\in I}\deg f < n \Rightarrow < (q-1)n$$

by assumption. Hence there exists a finite set T and $\lambda_i \in K$ such that

$$P = \sum_{i\in T}\lambda_i \prod_{j=1}^{n} x_j^{u_{ij}}$$

and for all $i \in T$, $\sum_{j=1}^{n} u_{ij} < (q-1)n$. Then

$$S(P) = \sum_{x\in K^n} P(x) \tag{1.1}$$

$$= \sum_{x\in K^n}\sum_{i\in T}\lambda_i \prod_{j=1}^{n} x_j^{u_{ij}} \tag{1.2}$$

$$= \sum_{i\in T}\lambda_i \sum_{x\in K^n}\prod_{j=1}^{n} x_j^{u_{ij}} \tag{1.3}$$

$$\tag{1.4}$$

Let $i \in T$ then there exists a k such that $u_{ik} < q-1$ so

$$\sum_{x\in K^n}\prod_{j=1}^{n} x_j^{u_{ij}} \tag{1.5}$$

$$= \sum_{x_1\in K}\cdots\sum_{x_n\in K}\prod_{j=1}^{n} x_j^{u_{ij}} \tag{1.6}$$

$$= \sum_{x_1\in K}\cdots\cancel{\sum_{x_k\in K}}\cdots\sum_{x_n\in K}\prod_{j\neq k} x_j^{u_{ij}}\sum_{x_k\in K} x_k^{u_{ik}} \tag{1.7}$$

$$= \sum_{x_1\in K}\cdots\cancel{\sum_{x_k\in K}}\cdots\sum_{x_n\in K}\prod_{j\neq k} x_j^{u_{ij}}0 \tag{1.8}$$

The last part using the power sum lemma. Hence $|V(I)| \overset{p}{=} S(P) = 0$ □

Corollary – Non-trivial vanishing
Suppose for all $f \in I \subseteq K[x1, \ldots, x_n]$ (finite),

$$\sum_{f\in I}\deg f < n$$

and $0 \in V(I)$ then $\exists x \in V(I) \setminus \{0\}$.

Proof. If $|V| = 1$ then $p \not| |V|$ which is a contradiction. Thus the vanishing is non-trivial. □

Definition – Homogeneous
$f \in K[x1, \dots, x_n]$ is homogeneous with degree m if all monomials are of degree m.

Corollary – Conics over a finite field
If $3 \leq n$ then if $f \in K[x1, \dots, x_n]$ is homogeneous with degree 2 then it has a non-trivial zero.

1.3 Quadratic reciprocity

Proposition – Exact sequence
If K is a finite field,

- If $\mathrm{Char}(K) = 2$ then all elements are square.
- If $\mathrm{Char}(K) \neq 2$ then the non-zero squares form a subgroup of index 2, and is the kernel of the group morphism $x \to x^{\frac{q-1}{2}}$ into $\langle -1 \rangle$.

I can't be bothered to make the exact sequence.

Proof.

- If $\mathrm{Char}(K) = 2$ then the Frobenius map $\sigma_2 : x \mapsto x^2$ is an automorphism of K. Hence the preimage of any element squares to that element.
- If $\mathrm{Char}(K) \neq 2$ then generate $K^* = \langle g \rangle$ since it is cyclic. The map $x \to x^{\frac{q-1}{2}}$ has kernel $\{x \in K \mid x \text{ square}\}$ since (writing any element as a multiple of g)

$$g^n \in \ker \Leftrightarrow g^{\frac{n(q-1)}{2}} = 1 \Leftrightarrow q - 1 \mid \frac{n(q-1)}{2} \Leftrightarrow n \text{ even} \Leftrightarrow x \text{ square}$$

  We check where the generator g is sent. If $g^{\frac{q-1}{2}} = 1$ then the order of g is less than $q-1$ which is a contradiction hence the image is non-trivial. Any element of the image of the map squares to 1 hence solves $x^2 - 1 = 0$, which only has two solutions in K. Thus the image is $\langle -1 \rangle$ and the index of the kernel is 2.

□

Definition – Legendre symbol
If p is prime that is not 2 and $x \in \mathbb{F}_p$ then

$$\left(\frac{x}{p}\right) := \begin{cases} x^{\frac{p-1}{2}} & , x \text{ unit} \\ 0 & , x = 0 \end{cases}$$

Check that for each p this is a homomorphism $\mathbb{F}_p \to \langle -1 \rangle$.

Definition – $\varepsilon(n)$
If $n \in \mathbb{Z}$ is odd

$$\varepsilon(n) := \frac{n-1}{2} (\mathrm{mod} 2)$$

Proposition – Computations

$$\begin{aligned}\left(\frac{1}{p}\right) =& 1 \\ \left(\frac{-1}{p}\right) =& (-1)^{\varepsilon(p)}\end{aligned}$$

Proposition – Quadratic reciprocity
Let $l \neq p$ be primes that aren't 2. Then

$$\left(\frac{l}{p}\right)\left(\frac{p}{l}\right) = (-1)^{\varepsilon(l)\varepsilon(p)}$$

Proof. Let w be order l element of Ω, the algebraic closure of $\mathbb{F}_p$. For $x \in \mathbb{F}_l$ write w^x to be w^r for any $r \in \mathbb{Z}$ such that $x = \overline{r} \in \mathbb{F}_l$ (independant of choice of r by $w^l = 1$). Let

$$y = \sum_{x \in \mathbb{F}_l} \left(\frac{x}{l}\right) w^x \in \Omega$$

We first show that $y^2 = (-1)^{\varepsilon(l)}\bar{l}$, where $\bar{l} \in \mathbb{F}_p$.

$$\begin{aligned}y^2 =& (\sum_{x \in \mathbb{F}_l} \left(\frac{x}{l}\right) w^x)(\sum_{y \in \mathbb{F}_l} \left(\frac{y}{l}\right) w^y) \\ =& \sum_{x \in \mathbb{F}_l} \sum_{y \in \mathbb{F}_l} \left(\frac{x}{l}\right) w^x \left(\frac{y}{l}\right) w^y \\ =& \sum_{x \in \mathbb{F}_l} \sum_{y \in \mathbb{F}_l} \left(\frac{xy}{l}\right) w^{x+y} \\ =& \sum_{u \in \mathbb{F}_l} \sum_{x \in \mathbb{F}_l} \left(\frac{x(u-x)}{l}\right) w^u\end{aligned}$$

Case on what x is:

$$
\begin{aligned}
x \neq 0 \Rightarrow \left(\frac{x(u-x)}{l}\right) = & \left(\frac{xu - x^2}{l}\right) \\
= & \left(\frac{x^2}{l}\right)\left(\frac{-1}{l}\right)\left(\frac{1-\frac{u}{x}}{l}\right) \\
= & x^{p-1}\left(\frac{-1}{l}\right)\left(\frac{1-\frac{u}{x}}{l}\right) \\
= & (-1)^{\varepsilon(l)}\left(\frac{1-\frac{u}{x}}{l}\right)
\end{aligned}
$$

If $x = 0$ then clearly $\left(\frac{x(u-x)}{l}\right) = 0$. Hence

$$
y^2 = \sum_{u \in \mathbb{F}_l} \sum_{x \in \mathbb{F}_l^*} (-1)^{\varepsilon(l)} \left(\frac{1-\frac{u}{x}}{l}\right) = (-1)^{\varepsilon(l)} \sum_{u \in \mathbb{F}_l} \sum_{x \in \mathbb{F}_l^*} \left(\frac{1-\frac{u}{x}}{l}\right)
$$

Given $x \neq 0$, case on what u is:

$$
\begin{aligned}
u = 0 \Rightarrow & \sum_{x \in \mathbb{F}_l^*} \left(\frac{1-\frac{u}{x}}{l}\right) \\
= & \sum_{x \in \mathbb{F}_l^*} \left(\frac{1}{l}\right) \\
= & \sum_{x \in \mathbb{F}_l^*} 1 \\
= & l - 1
\end{aligned}
$$

$$
\begin{aligned}
u \neq 0 \Rightarrow & \sum_{x \in \mathbb{F}_l^*} \left(\frac{1-\frac{u}{x}}{l}\right) \\
= & \sum_{x \in F_l^*} \left(\frac{1-\frac{1}{x}}{l}\right) \\
= & \sum_{s \in \mathbb{F}_l^*} \left(\frac{1-s}{l}\right) \\
= & \sum_{s \in \mathbb{F}_l \setminus \{1\}} \left(\frac{s}{l}\right) \\
= & \sum_{s \in \mathbb{F}_l} \left(\frac{s}{l}\right) - \left(\frac{1}{l}\right) \\
= & -1
\end{aligned}
$$

Since the index of the kernel of $\left(\frac{\star}{l}\right)$ is 2, and the cosets have equal cardinality. Hence

$$\begin{aligned} y^2(-1)^{\varepsilon(l)} &= \sum_{u\in\mathbb{F}_l}\sum_{x\in\mathbb{F}_l^*}\left(\frac{1-\frac{u}{x}}{l}\right) \\ &= \bar{l}-1-\sum_{u\in\mathbb{F}_l^*} w^u \\ &= \bar{l}-(1+w+w^2+\cdots+w^l) \end{aligned}$$

since l is prime. Note that $0 = w^l - 1 = (w+1)(1+w+\cdots+w^l)$. Hence $1+w+\cdots+w^l = 0$ and $y^2 = (-1)^{\varepsilon(l)}\bar{l}$. Next we show that $y^{p-1} = \left(\frac{p^{-1}}{l}\right)$.

$$\begin{aligned} y^p &= \sum_{x\in\mathbb{F}_l}\left(\frac{x}{l}\right)^p w^x p && \text{'Freshman's dream'} \\ &= \sum_{x\in\mathbb{F}_l}\left(\frac{x}{l}\right) w^x p && \left(\frac{x}{l}\right) = \pm 1 \text{ and } p \text{ is odd} \\ &= \sum_{z\in\mathbb{F}_l}\left(\frac{zp^{-1}}{l}\right) w^z \\ &= \left(\frac{p^{-1}}{l}\right)\left(\sum_{z\in\mathbb{F}_l}\left(\frac{z}{l}\right) w^z\right) \\ &= \left(\frac{p^{-1}}{l}\right) y \end{aligned}$$

Hence

$$y^{p-1} = \left(\frac{p^{-1}}{l}\right) = (\left(\frac{pl}{)}\right)^{-1}$$

thus

$$\begin{aligned} \left(\frac{l}{p}\right)\left(\frac{p}{l}\right) &= \left(\frac{l}{p}\right) y^{1-p} \\ &= \left(\frac{l}{p}\right)(y^2)^{\frac{1-p}{2}} \\ &= \left(\frac{l}{p}\right)((-1)^{\varepsilon(l)}\bar{l})^{\frac{1-p}{2}} \\ &= \left(\frac{l}{p}\right)(\left(\frac{(-1)^{\varepsilon(l)}l}{p}\right))^{-1} \\ &=(\left(\frac{(-1)^{\varepsilon(l)}}{p}\right))^{-1} \\ &=(-1)^{\varepsilon(l)\varepsilon(p)} \end{aligned}$$

$\square$

1.4 Quadratic reciprocity

Proposition – Exact sequence
If K is a finite field,

- If $\mathrm{Char}(K) = 2$ then all elements are square.
- If $\mathrm{Char}(K) \neq 2$ then the non-zero squares form a subgroup of index 2, and is the kernel of the group morphism $x \to x^{\frac{q-1}{2}}$ into $\langle -1 \rangle$.

I can't be bothered to make the exact sequence.

Proof.

- If $\mathrm{Char}(K) = 2$ then the Frobenius map $\sigma_2 : x \mapsto x^2$ is an automorphism of K. Hence the preimage of any element squares to that element.
- If $\mathrm{Char}(K) \neq 2$ then generate $K^* = \langle g \rangle$ since it is cyclic. The map $x \to x^{\frac{q-1}{2}}$ has kernel $\{x \in K \mid x \text{ square}\}$ since (writing any element as a multiple of g)

$$g^n \in \ker \Leftrightarrow g^{\frac{n(q-1)}{2}} = 1 \Leftrightarrow q-1 \mid \frac{n(q-1)}{2} \Leftrightarrow n \text{ even} \Leftrightarrow x \text{ square}$$

We check where the generator g is sent. If $g^{\frac{q-1}{2}} = 1$ then the order of g is less than $q-1$ which is a contradiction hence the image is non-trivial. Any element of the image of the map squares to 1 hence solves $x^2 - 1 = 0$, which only has two solutions in K. Thus the image is $\langle -1 \rangle$ and the index of the kernel is 2.

□

Definition – Legendre symbol
If p is prime that is not 2 and $x \in \mathbb{F}_p$ then

$$\left(\frac{x}{p}\right) := \begin{cases} x^{\frac{p-1}{2}} & , x \text{ unit} \\ 0 & , x = 0 \end{cases}$$

Check that for each p this is a homomorphism $\mathbb{F}_p \to \langle -1 \rangle$.

Definition – $\varepsilon(n)$
If $n \in \mathbb{Z}$ is odd

$$\varepsilon(n) := \frac{n-1}{2} (\mathrm{mod} 2)$$

Proposition – Computations

$$\begin{aligned}\left(\frac{1}{p}\right) =&1\\ \left(\frac{-1}{p}\right) =&(-1)^{\varepsilon(p)}\end{aligned}$$

Proposition – Quadratic reciprocity
Let $l \neq p$ be primes that aren't 2. Then

$$\left(\frac{l}{p}\right)\left(\frac{p}{l}\right) = (-1)^{\varepsilon(l)\varepsilon(p)}$$

Proof. Let w be order l element of Ω, the algebraic closure of $\mathbb{F}_p$. For $x \in \mathbb{F}_l$ write w^x to be w^r for any $r \in \mathbb{Z}$ such that $x = \overline{r} \in \mathbb{F}_l$ (independant of choice of r by $w^l = 1$). Let

$$y = \sum_{x \in \mathbb{F}_l} \left(\frac{x}{l}\right) w^x \in \Omega$$

We first show that $y^2 = (-1)^{\varepsilon(l)}\bar{l}$, where $\bar{l} \in \mathbb{F}_p$.

$$\begin{aligned}y^2 =&(\sum_{x\in\mathbb{F}_l}\left(\frac{x}{l}\right) w^x)(\sum_{y\in\mathbb{F}_l}\left(\frac{y}{l}\right) w^y)\\ =&\sum_{x\in\mathbb{F}_l}\sum_{y\in\mathbb{F}_l}\left(\frac{x}{l}\right) w^x \left(\frac{y}{l}\right) w^y\\ =&\sum_{x\in\mathbb{F}_l}\sum_{y\in\mathbb{F}_l}\left(\frac{xy}{l}\right) w^{x+y}\\ =&\sum_{u\in\mathbb{F}_l}\sum_{x\in\mathbb{F}_l}\left(\frac{x(u-x)}{l}\right) w^u\end{aligned}$$

Case on what x is:

$$\begin{aligned}x \neq 0 \Rightarrow \left(\frac{x(u-x)}{l}\right) =& \left(\frac{xu - x^2}{l}\right)\\ =& \left(\frac{x^2}{l}\right)\left(\frac{-1}{l}\right)\left(\frac{1-\frac{u}{x}}{l}\right)\\ =& x^{p-1}\left(\frac{-1}{l}\right)\left(\frac{1-\frac{u}{x}}{l}\right)\\ =& (-1)^{\varepsilon(l)}\left(\frac{1-\frac{u}{x}}{l}\right)\end{aligned}$$

If $x = 0$ then clearly $\left(\frac{x(u-x)}{l}\right) = 0$. Hence

$$y^2 = \sum_{u\in\mathbb{F}_l}\sum_{x\in\mathbb{F}_l^*}(-1)^{\varepsilon(l)}\left(\frac{1-\frac{u}{x}}{l}\right) = (-1)^{\varepsilon(l)}\sum_{u\in\mathbb{F}_l}\sum_{x\in\mathbb{F}_l^*}\left(\frac{1-\frac{u}{x}}{l}\right)$$

Given $x \neq 0$, case on what u is:

$$\begin{aligned} u = 0 \Rightarrow \sum_{x\in\mathbb{F}_l^*}\left(\frac{1-\frac{u}{x}}{l}\right) \\ &= \sum_{x\in\mathbb{F}_l^*}\left(\frac{1}{l}\right) \\ &= \sum_{x\in\mathbb{F}_l^*} 1 \\ &= \bar{l} - 1 \end{aligned}$$

$$\begin{aligned} u \neq 0 \Rightarrow \sum_{x\in\mathbb{F}_l^*}\left(\frac{1-\frac{u}{x}}{l}\right) \\ &= \sum_{x\in F_l^*}\left(\frac{1-\frac{1}{x}}{l}\right) \\ &= \sum_{s\in\mathbb{F}_l^*}\left(\frac{1-s}{l}\right) \\ &= \sum_{s\in\mathbb{F}_l\setminus\{1\}}\left(\frac{s}{l}\right) \\ &= \sum_{s\in\mathbb{F}_l}\left(\frac{s}{l}\right) - \left(\frac{1}{l}\right) \\ &= -1 \end{aligned}$$

Since the index of the kernel of $\left(\frac{\star}{l}\right)$ is 2, and the cosets have equal cardinality. Hence

$$\begin{aligned} y^2(-1)^{\varepsilon(l)} &= \sum_{u\in\mathbb{F}_l}\sum_{x\in\mathbb{F}_l^*}\left(\frac{1-\frac{u}{x}}{l}\right) \\ &= \bar{l} - 1 - \sum_{u\in\mathbb{F}_l^*} w^u \\ &= \bar{l} - (1 + w + w^2 + \cdots + w^l) \end{aligned}$$

since l is prime. Note that $0 = w^l - 1 = (w+1)(1+w+\cdots+w^l)$. Hence $1+w+\cdots+w^l = 0$ and $y^2 = (-1)^{\varepsilon(l)}\bar{l}$.

Next we show that $y^{p-1} = \left(\frac{p^{-1}}{l}\right)$.

$$\begin{aligned}
y^p &= \sum_{x\in\mathbb{F}_l} \left(\frac{x}{l}\right)^p w^x p && \text{'Freshman's dream'}\\
&= \sum_{x\in\mathbb{F}_l} \left(\frac{x}{l}\right) w^x p && \left(\frac{x}{l}\right) = \pm 1 \text{ and } p \text{ is odd}\\
&= \sum_{z\in\mathbb{F}_l} \left(\frac{zp^{-1}}{l}\right) w^z \\
&= \left(\frac{p^{-1}}{l}\right) \left(\sum_{z\in\mathbb{F}_l} \left(\frac{z}{l}\right) w^z\right) \\
&= \left(\frac{p^{-1}}{l}\right) y
\end{aligned}$$

Hence

$$y^{p-1} = \left(\frac{p^{-1}}{l}\right) = (\left(\frac{pl}{)}\right)^{-1}$$

thus

$$\begin{aligned}
\left(\frac{l}{p}\right)\left(\frac{p}{l}\right) &= \left(\frac{l}{p}\right) y^{1-p} \\
&= \left(\frac{l}{p}\right) (y^2)^{\frac{1-p}{2}} \\
&= \left(\frac{l}{p}\right) ((-1)^{\varepsilon(l)}\bar{l})^{\frac{1-p}{2}} \\
&= \left(\frac{l}{p}\right) (\left(\frac{(-1)^{\varepsilon(l)} l}{p}\right))^{-1} \\
&= (\left(\frac{(-1)^{\varepsilon(l)}}{p}\right))^{-1} \\
&= (-1)^{\varepsilon(l)\varepsilon(p)}
\end{aligned}$$

□

Chapter 2

p-adic Fields

2.1 p-adic Integers and Rationals

Definition – Projective system A
Define a contravariant functor $A : (\mathbb{N}, \leq) \to \mathbf{Ring}$ such that for each n

$$A_n := \mathbb{Z}/p^n\mathbb{Z} \quad \text{and} \quad \pi_n : \mathbb{Z} \to A_n \text{ is the projection}$$

and for any n such that $1 \leq n$, there exists a surjective ring morphism $\phi_n : A_n \to A_{n-1}$ such that $\phi_n \circ \pi_n = \pi_{n-1}$ and $\ker(\phi_n) = p^{n-1}A_n$.

Exercise. *Check that such a ϕ_n exists.*

Definition – p-adic integers
Let

$$\mathbb{Z}_p = \{x \in \prod_{n \in \mathbb{N}} A_n \mid (\forall n \in \mathbb{N}, x_n \in A_n) \wedge (\forall n > 0, \phi_n(x_n) = x_{n-1})\}$$

Define addition and multiplication pointwise. Verify that this $\mathbb{Z}_p$ is a ring with $0 = (0)_{n\in\mathbb{N}}$ and $1 = (1)_{n\in\mathbb{N}}$.

For each $n \in \mathbb{N}$ let $\varepsilon_n : \mathbb{Z}_p \to A_n$ be the ring morphisms mapping $x \mapsto x_n$. Note that by definition $\phi_n \circ \varepsilon_n = \varepsilon_{n-1}$.

In addition, provide each A_n with the discrete toplogy, giving $\prod_{n\in\mathbb{N}} A_n$ the product topology and $\mathbb{Z}_n$ the subset topology.

Proposition – $\mathbb{Z}_p$ is compact

Since each A_n is finite, each A_n is compact. Hence by Tychonoff's theorem the product is compact. Since closed in compact is compact we just need to show that $\mathbb{Z}_p$ is closed.

We want to write $\mathbb{Z}_p$ as the intersection of closed sets

$$D_k := \left\{ x \in \prod_{n\in\mathbb{N}} A_n \mid \phi_k(x_k) = x_{k-1} \right\}$$

for $k \in \mathbb{N}$. Clearly

$$\bigcap_{k\in\mathbb{N}} D_k = \mathbb{Z}_p$$

and

$$D_k = \bigcup_{x_{k-1}\in A_{k-1}} \left(\varepsilon_{k-1}^{-1}(x_{k-1}) \cap \bigcup \left\{ \varepsilon_k^{-1}(x_k) \mid x_k \in A_k \wedge \phi_k(x_k) = x_{k-1} \right\} \right)$$

Since each $\{x_k\}$ is closed in A_k, each preimage $\varepsilon_k^{-1}(x_k)$ is closed. Thus the finite union of the preimages

$$\bigcup \left\{ \varepsilon_k^{-1}(x_k) \mid x_k \in A_k \wedge \phi_k(x_k) = x_{k-1} \right\}$$

is closed. Since each $\{x_{k-1}\}$ is closed in A_{k-1}, each preimage $\varepsilon_{k-1}^{-1}(x_{k-1})$ is closed. Thus intersection

$$\left(\varepsilon_{k-1}^{-1}(x_{k-1}) \cap \bigcup \left\{ \varepsilon_k^{-1}(x_k) \mid x_k \in A_k \wedge \phi_k(x_k) = x_{k-1} \right\} \right)$$

is closed. Hence the finite union is closed and D_k is closed. Arbitrary intersection of closed is closed so $\mathbb{Z}_p$ is closed and thus compact.

Proposition – Universal property of $\mathbb{Z}_p$

Suppose R is a ring with ring morphisms $\rho_n : R \to A_n$ for each $n \in \mathbb{N}$ such that for each $n > 0$, $\phi_n \circ \rho_n = \rho_{n-1}$. Then there exists a unique ring morphism $f : R \to \mathbb{Z}_p$ such that for each n, $\varepsilon_n \circ f = \rho_n$.

Proof. If there exists such a map then it is unique: suppose f, g both satisfy the given properties. Then for any n and any $a \in R$ $\varepsilon_n \circ f(a) = \rho_n(a) = \varepsilon_n \circ g(a)$. Thus $f(a) = g(a)$, by the property of products (if they agree on all the projections they are equal).

For existance we let $a \in R$ and consider the set

$$\bigcap_{n\in\mathbb{N}} \varepsilon_n^{-1} \circ \rho_n(a)$$

show that it has cardinality 1, and let f map a to this unique element. If $x, y \in \bigcap_{n\in\mathbb{N}} \varepsilon_n^{-1} \circ \rho_n(a)$ then for any $n \in \mathbb{N}$, $\varepsilon_n(x) = \rho_n(a) = \varepsilon_n(y)$. Thus $a = b$ by the property of products. Hence the cardinality is ≤ 1.

To show that the set is non-empty, take $x = (\rho_n(a))_{n\in\mathbb{N}}$. This is in $\mathbb{Z}_p$ since for each $n > 0$, $\phi_n \circ \rho_n(a) = \rho_{n-1}(a)$. Also it is in the intersection since for each n, $\varepsilon_n(x) = \rho_n(a)$. Hence the cardinality is 1. Hence f is well-defined and for all $n \in \mathbb{N}$, $\varepsilon_n \circ f = \rho_n$.

For any n,

$$\varepsilon_n \circ f(a+b) = \rho_n(a+b) = \rho_n(a) + \rho_n(b) = \varepsilon_n \circ f(a) + \varepsilon_n \circ f(b) = \varepsilon_n(f(a) + f(b))$$

Hence by property of products $f(a+b) = f(a) + f(b)$ and similarly for multiplication. Note that for any n, $\varepsilon_n \circ f(1) = \rho_n(1) = 1$. Hence $f(1) = 1$. Thus f is a ring morphism. $\square$

Corollary – $\mathbb{Z}$ injects into $\mathbb{Z}_p$
Then there exists a unique injective ring morphism $\iota : \mathbb{Z} \to \mathbb{Z}_p$ such that for each n, $\varepsilon_n \circ \iota = \pi_n$.

Proof. By the previous theorem the morphism exists and is unique. It must send $1 \mapsto 1$ hence $\iota(x) = 0$ would imply $\pi_n(x) = \varepsilon_n \circ \iota(x) = 0$ for all $n \in \mathbb{N}$. Hence for any $n \in \mathbb{N}$, $p^n \mid x$. Thus $x = 0$. $\square$