Modular forms modulo 2

Paul Dubois

February 9, 2020

Abstract

We are interested in Modular forms modulo 2, and computing thing about it. [temporary abstract]

Key words that should appear: Modular forms; Mod 2; Duality of definitions; Governing fields; Frobenian map?; Exact computations;

Contents

1 Modular forms

1.1 Modular forms of level 1

We will denote by $\mathbb{H}$ the upper half plane.

We say that a complex function f on the upper half plane is weakly modular of weight $2k$ if f is meromorphic on $\mathbb{H}$ and

$$f(z) = (cz+d)^{-2k} f\left(\frac{az+b}{cz+d}\right) \qquad \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}).$$

A property of $SL_2(\mathbb{Z})$ is that when we define

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ and } T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

then $SL_2(\mathbb{Z})$ is generated by S and T (**?** , p.1-2).

From that property, we can derive an alternative definition of weakly modular functions: f is weakly modular of weight $2k$ if f is meromorphic on $\mathbb{H}$ and $f(z+1) = f(z)$ and $f(-1/z) = z^k f(z)$ for all $z \in \mathbb{Z}$.

Moreover, we also define a function $f : \mathbb{H} \to \mathbb{C}$ to be modular of weight $2k$ if f is holomorphic on $\mathbb{H}$ and f is weakly modular.

Lastly, we say that a function $f : \mathbb{H} \to \mathbb{C}$ is a modular form of weight $2k$ if f is holomorphic at ∞ and f is modular.

It is easy to check, from definition, that we can add modular forms together, as well as multiply them by a complex:

- $f_1(z) + f_2(z)$ is modular of weight $2k$ if $f_1(z)$ and $f_2(z)$ are modular of weight $2k$.
- $\lambda f(z)$ is modular of weight $2k$ if $f(z)$ is.

Therefore, modular forms of weight $2k$ over $\mathbb{C}$ form a space. We denote it M_k.

It is also possible to multiply modular forms, in which case the weights adds on: If $f_1(z)$ & $f_2(z)$ are modular of respective weights $2k_1$ & $2k_2$, then $f_1(z)f_2(z)$ is modular of weight $2k_1 + 2k_2$

We deduce that we can take powers of modular forms, and the weight is then multiplied by the power: If $f(z)$ is modular of weight $2k$, then $f^n(z)$ is modular of weight $2k * n$ (with $n \in \mathbb{N}$).

1.2 Typical Modular Forms

1.2.1 Eisenstein series G_k

The most famous class of modular forms is probably the Eisenstein series, usually denoted G_k. We define them as follows(**?** , Examples of Modular Forms of Level 1):

$$G_k(z) = \sum_{(m,n)\in\mathbb{Z}^2\setminus\{(0,0)\}} \frac{1}{(mz+n)^{2k}}$$

for $k \geq 2$.

It is easy to check that G_k are modular of weight $2k$(**?** , Proposition 2.1), as:

$$G_k(z+1) = G_k(z)$$

(using $(m, n+m) \to (m, n)$, an invertible map)

$$G_k(-1/z) = z^k G_k(z)$$

(using $(m, -n) \to (m, n)$, an invertible map).

It is pleasant to remark that (**?** , Proposition 2.2)

$$G_k(\infty) = \sum_{n \in \mathbb{Z}^*} \frac{1}{n^{2k}} = 2\zeta(2k)$$

. Where $\zeta(k)$ is Riemann Zeta function. The values of this function are well known on positive even numbers, and we deduce (**?** , p.194):

$$G_k(\infty) = 2\zeta(2k) = \frac{(2\pi)^{2k}}{(2k)!} B_k$$

with $B_k = (-1)^{k+1} b_{2k}$ where b_k are Bernoulli's numbers.

1.2.2 Δ

We will be interested in one main modular form in the rest of this article: Δ. We define Δ in terms of G_k as follows(**?** , p.84):

$$\Delta = g_2^3 - 27g_3^2 \in M_6^0 \qquad \text{with } g_2 = 40G_2 \text{ and } g_3 = 140G_3$$

As g_2^3 is modular of weight $4 * 3 = 12$ and g_3^2 of weight $6 * 2 = 12$, Δ is modular of weight 12.

Now, using $G_2(\infty) = 2\zeta(4) = \frac{\pi^4}{45}$ and $G_3(\infty) = 2\zeta(6) = \frac{2\pi^4}{945}$, we get $\Delta(\infty) = \left(\frac{4\pi^4}{3}\right)^3 - \left(\frac{8\pi^4}{27}\right)^2 = 0$.

1.3 Cusp Forms

A function $f : \mathbb{H} \to \mathbb{C}$ that is a modular form may in addition be a cusp form, if $f(\infty) = 0$. We will denote the space of modular cusp forms of weight $2k$ over $\mathbb{C}$ by M_k^0.

It is useful to note $G_k(\infty) = \sum_{n \in \mathbb{N}^*} \frac{2}{n^{2k}} > 2$ and in particular, $G_k(\infty) \neq 0$, so G_k are *not* cusp forms for any k. As we have shown it before, $\Delta(\infty) = 0$, so Δ is a modular cusp form of weight 12, so $\Delta \in M_6^0$. Using tools from complex analysis, we can prove that Δ has only one zero (at infinity), which has order one(**?** , p.88).

We have the following relation:

Theorem 1. *$M_k \cong M_k^0 \oplus \mathbb{C}.G_k \qquad \forall k \geq 2$.(**?** , p.88)*

Proof. We let $\Phi : M_k \to \mathbb{C}$ such that if $f \in M_k$, $\Phi(f) = f(\infty)$.

Now, we have $\text{Ker}(\Phi) = M_k^0$, therefore, by the 1st Isomorphism Theorem, ${}^{M_k}/_{M_k^0} \cong \text{Im}(\Phi) \subseteq \mathbb{C}$.

Note that $G_k \in M_k$, and $G_k(\infty) = \sum_{n \in \mathbb{Z}^*} \frac{1}{n^{2k}} \neq 0$, so $G_k \notin M_k^0$. As $G_k \neq 0$, $\dim({}^{M_k}/_{M_k^0}) \geq 1$ and $\text{Im}(\Phi) = \mathbb{C}$. Thus, $G_k \in M_k$
M_k^0

Finally, we have $M_k \cong M_k^0 \oplus \mathbb{C}.G_k$ if $k \geq 2$. (The above argument fails for $k < 2$ as G_k is not well defined any more.) □

Therefore, the dimensions of M_k and M_k^0 are closely linked.

1.4 Dimensions of Spaces of Modular Forms

The fact that multiplying two modular forms gives a function that remains modular yields that we may map a set of modular forms to an other.

Theorem 2. *$M_{k-6} \cong M_k^0$.(**?** , p.88)*

Proof. We let $\Phi : M_{k-6} \to M_k^0$ such that if $f \in M_k$, $\Phi(f)(z) = \Delta(z)f(z)$.

This is well defined as if f has weight $2(k-6)$, $\Delta.f$ has weight $2k$ since Δ has weight 12. As Δ is a cusp from, $\Delta.f$ will also be a cusp form.

From definition, Φ is clearly homomorphic.

Now, if $g \in M_k^0$, we may define $\Psi : M_k^0 \to M_{k-6}$ such that $\Psi(g)(z) = {}^{g(z)}/_{\Delta(z)}$

This is well defined as if g has weight $2k$, $\Delta.f$ has weight $2k$ since Δ has weight 12. As Δ is a cusp from, $\Delta.f$ will also be a cusp form.

This is well defined as Δ has only one zero, at infinity, where g also has a zero (as g is a cusp form). The weights agree again as well.

It is then easy to remark that $\Psi = \Phi^{-1}$. So Φ is bijective, and thus isomorphic.

Finally, we have $M_{k-6} \cong M_k^0$. □

This theorem, combined with the previous one is very powerful: it shows that there must be a pattern (of 6) in the sequence of dimensions $\dim(M_k)$ and $\dim(M_k^0)$ for $k \geq 2$. We have $M_k \cong M_k^0 \oplus \mathbb{C}.G_k \cong M_{k-6} \oplus \mathbb{C}.G_k$, so $\dim(M_k) = \dim(M_{k-6}) + 1$ when $k \geq 2$. Thus, if we compute the dimensions of M_0, M_1, M_2, M_3, M_4, M_5, we can extrapolate dimensions of M_k and M_k^0 for all k.

Using complex analysis techniques again, we have:

- $\dim(M_k) = 0 \quad k < 0$
- $\dim(M_1) = 0$
- $\dim(M_0) = \dim(M_2) = \dim(M_3) = \dim(M_4) = \dim(M_5) = 1$

In the case $k = 0$, $\dim(M_0) = 1$. As $f(z) = 1$ is clearly a modular from of weight 0, $\{1\}$ is a basis for M_0. We deduce $\dim(M_k^0) = 0$ as 1 is clearly not a cusp form. In the case $k = 1$, $\dim(M_1) = 0$, which makes $\dim(M_1^0) = 0$ automatically. (Cases $k < 0$ are similar to $k = 1$.)

Other cases may be derived directly from the relations (using induction to get general formulas), and we obtain:

Space	$k < 0$	$k \geq 0,\ k \equiv 1 \mod 6$	$k \geq 0,\ k \not\equiv 1 \mod 6$
$\dim(M_k)$	0	$\lfloor k/6 \rfloor$	$\lfloor k/6 \rfloor + 1$
$\dim(M_k^0)$	0	$\max\{0, \lfloor k/6 \rfloor - 1\}$	$\lfloor k/6 \rfloor$

Note that the max is taken only to avoid negative dimensions.

1.5 Fourier Expansion

1.5.1 Definition

To study such function, we use Fourier Expansion. In the case of f being a modular form of weight $2k$, a Fourier Expansion is a representation of f as a power series of $e^{2\pi i n z}$ i.e.

$$f(z) = \sum_{n \in \mathbb{Z}} a_n(f) e^{2\pi i n z}.$$

We usually denote $q = e^{2\pi i z}$ so that $q^n = e^{2\pi i n z}$ and the Fourier expansion of f become

$$f(q) = \sum_{n \in \mathbb{Z}} a_n(f) q^n.$$

When in this form, we may as well call it the q expansion.

1.5.2 Typical Modular Forms Fourier Expansion

Fourier Expansions of G_k The modular forms G_k have the following q expansion(**?** , p.92):

$$G_k(q) = 2\zeta(2k) + 2\frac{(2\pi i)^{2k}}{(2k-1)!} \sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n$$

with $\sigma_s(n) = \sum_{d|n} d^s$, for $k \geq 4$.

Fourier Expansion of Δ We also have(**?** , p.95):

$$\Delta(q) = (2\pi)^{12} q \prod_{n=1}^{\infty} (1 - q^n)^{24}$$

1.6 A Basis for Modular Forms

The set of modular forms that are weight $2k$ in fact form a vector space (we can add modular forms together, and multiply them with a constant) over the complex numbers. One may ask then a basis for this vector space.

We would like to find a basis for each set M_k. It turns out that the modular forms G_2 and G_3 introduced before in fact generate a basis for all M_k. It is not obvious and may in fact seems wrong at a first stage: G_2 and G_3 are modular forms of weight 4 and 6, whereas M_k in general have modular forms of weight $2k$. However, by taking combinations of G_2 and G_3, we may obtain modular forms of any weight $2k$. It is important to remember that when multiplied, the weight of modular forms add up.

Theorem 3. *The set $S = \{G_2^a G_3^b | a, b \in \mathbb{N}, 2a + 3b = k\}$*[1] *is a basis for M_k.(**?** , Theorem 2.17)*

Proof. Of course, the cases when $\dim(M_k) = 0$ (for $k < 0$ and $k = 1$) are trivial, as the basis is empty, and $2a + 3b = k$ has no solution for $a, b \in \mathbb{N}$.

To show S is a basis, we need it to span M_k and to be linearly independent.

We start with spanning, and we proceed by induction on k, with step 6.

As $\dim(M_k) = 1$ for $k = 0, 2, 3, 4, 5, 7$, and the equation $2a + 3b = k$ has exactly one solution for $a, b \in \mathbb{N}$ (namely $(a, b) = (0, 0), (1, 0), (0, 1), (2, 0), (1, 1), (2, 1)$), S has only one element, which must be the basis.

Now, for $k > 7$, take some $a, b \in \mathbb{N}$ such that $2a + 3b = k$. Let $f \in M_k$, and $g = G_2^a G_3^b \in M_k$. $g(\infty) \neq 0$ as none of G_2 or G_3 is a cusp form. So there must be a complex λ such that $f - \lambda g$ is a cusp form. Then $f - \lambda g \in M_k \cong M_{k-6}^0$ and we can find a $h \in M_{k-6}^*$ such that $h.\Delta = f - \lambda g$.

By induction, h must be a polynomial of G_2 and G_3; by definition, Δ is one as well (note that yet, we don't put any restriction on powers of G_2 and G_3, other then being positive integers). Therefore, $f = \Delta.h + \lambda g$ is a polynomial of G_2 and G_3. From the fact that $f \in M_k$ (i.e. f has weight $2k$), terms of f as a polynomial of G_2 and G_3 have the from $G_2^a G_3^b$ with $2a + 3b = k$.

We now want to show linear independence, we proceed by contradiction.

Suppose there is a non-trivial linear relation of terms $G_2^a G_3^b$. We can multiply it by suitable G_2 and G_3 so that all terms have the form $2a + 3b = k \equiv 0 \mod 12$. Then, we can divide all terms by G_3^2, witch gives us that there is a polynomial for which G_2^3/G_3^2 is a root. In particular, this polynomial is constant when G_2^3/G_3^2 is plugged. This contradicts the fact that q expansion of G_2^3/G_3^2 is not constant. □

This set of makes to be a basis, and one may even find it pleasant: given the two modular forms G_2 and G_3, this set generates all the modular forms of weight $2k$ that we could think of, if we only knew these two modular forms.

1.7 Hecke Operators

We define the Hecke operators for a modular form f as follows(**?** , p.100):

$$T(n)f(z) = n^{2k-1} \sum_{a \geq 1,\, ad=n,\, 0 \leq b < d} d^{-2k} f\left(\frac{az + b}{d}\right)$$

with $n \in \mathbb{N}$.

We can check that $T(n)f$ is modular if f is (as the sum of modular forms).

[1] The set of naturals $\mathbb{N}$ is taken to start from 0.

We may as well write $T(n)f$ as a Fourier Expansion of $q = e^{2\pi i z}$ as follows(**?** , p.100):

$$T(n)f(z) = \sum_{m\in\mathbb{Z}} \gamma(m)q^m \quad \text{with} \quad \gamma(z) = \sum_{a|(n,m),\, a\geq 1} a^{2k-1}c\left(\frac{mn}{a^2}\right)$$

$$\text{For modular forms } f \text{ s.t. } f(z) = \sum_{n\in\mathbb{Z}} \alpha(n)q^n$$

2 Modular Forms Modulo Two

2.1 Strategy to Reduce Modulo Two

It is not trivial, at this point, why and how we can reduce modulo two modular forms, objects that have coefficients in $\mathbb{C}$. In general, reduction modulo a number is only possible with whole numbers (integers). We would like to reduce modulo two coefficients of the Fourier series for modular forms. But at the moment, they lie in $\mathbb{C}$.

In fact, we will introduce a new basis for the modular forms: the so called Miller Basis. The coefficients of all the forms in this basis are integers. It is then possible to consider the space of modular forms over $\mathbb{Z}$ instead of $\mathbb{C}$. Once this is done, we will reduce all the newly integers coefficients modulo 2.

In this section, we will denote all object reduced with an $\overline{\text{over-line}}$: $f \to \overline{f}$; $c \to \overline{c}$; $T_n \to \overline{T_n}$.

2.2 Integer Basis

2.2.1 Normalisation of Typical Modular Forms

Normalisation of Eisenstein series G_k We first recall the formula for q extension of G_k and the one for $\zeta(2k)$:

$$G_k(q) = 2\zeta(2k) + 2\frac{(2\pi i)^{2k}}{(2k-1)!}\sum_{n=1}^{\infty}\sigma_{2k-1}(n)q^n$$

and

$$2\zeta(2k) = \frac{(2\pi)^{2k}}{(2k)!}B_k$$

so overall:

$$G_k(q) = \frac{(2\pi)^{2k}}{(2k)!}B_k + 2\frac{(2\pi i)^{2k}}{(2k-1)!}\sum_{n=1}^{\infty}\sigma_{2k-1}(n)q^n$$

We would like to normalize this series, so that the coefficients become integers, so that we can ultimately reduce them modulo two. Right now, coefficients are rational.

As we want to keep the series modular with same weight, the only tool we have to normalize the series is multiplication by a constant. The normalization is a crucial point: If we multiply by 2 all coefficients of a modular form that already lie in $\mathbb{Z}$, the reduction $\mod 2$ will always give zero.

First, let's normalize the series to have particular values on some coefficients of interest. There are two justified ways to do so: normalize to have constant coefficient set to one, and to have q coefficient is set to one. We will introduce both: Let E_k be such that:

$$E_k.2\zeta(2k) = G_k$$

so that

$$E_k = 1 + (-1)^k\frac{4k}{B_k}\sum_{n=1}^{\infty}\sigma_{2k-1}(n)q^n.$$

E_k then has constant coefficient set to one.

Let F_k be such that:

$$F_k.\left(2\frac{(2\pi i)^{2k}}{(2k-1)!}\right) = G_k$$

so that

$$F_k = (-1)^k\frac{B_k}{4k} + \sum_{n=1}^{\infty}\sigma_{2k-1}(n)q^n.$$

F_k then has q coefficient set to one (as $\sigma_{2k-1}(1) = 1$).

Clearly, the coefficients of this expansion remain in $\mathbb{Q}$ at least, and we will show that for some specific k, the coefficients lie in fact in $\mathbb{Z}$. Both F_k and E_k are interesting, but for our purpose (reducing modulo two), we will use E_k. Note that E_k are normalized versions of Eisenstein series G_k, but in literature, both are called Eisenstein series see (**?** , p.6) for example.

Normalisation of $\mathit{\Delta}$ Again, we recall the formula for q extension of $\mathit{\Delta}$:

$$\mathit{\Delta}(q) = (2\pi)^{12} q \prod_{n=1}^{\infty} (1 - q^n)^{24}$$

Again, we want to normalize the series so that the first coefficient is one. As there is no constant coefficients, we will normalize it so that the q coefficient becomes 1. Therefore, we define $\mathit{\Delta} = (2\pi)^{12}.\Delta$, so explicitly:

$$\Delta(q) = q \prod_{n=1}^{\infty} (1 - q^n)^{24}$$

Defined that way, Δ is known as the discriminant modular form.

Clearly, the coefficients in expansion of Δ are integers (which we can reduce modulo two).

2.2.2 Miller Basis

Basis with Integer Coefficients (in Fourier Series) Applying normalization $G_k \to E_k$ above for $k = 2, 3$, we get:

$$\begin{aligned} E_2 &= 1 + \frac{8}{B_2} \sum_{n=1}^{\infty} \sigma_3(n) q^n \qquad B_2 = \frac{1}{30} \\ &= 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n \end{aligned}$$

and

$$\begin{aligned} E_3 &= 1 - \frac{12}{B_3} \sum_{n=1}^{\infty} \sigma_5(n) q^n \qquad B_3 = \frac{1}{42} \\ &= 1 - 504 \sum_{n=1}^{\infty} \sigma_5(n) q^n \end{aligned}$$

Now, we have shown that $\{G_2^a G_3^b | 2a + 3b = k\}$ is a basis for modular forms of weight $2k$ over the complex (see 1.6). As $E_2 = \lambda G_2$, $\lambda \in \mathbb{C}$ and $E_3 = \mu G_3$, $\mu \in \mathbb{C}$, we have that $\{E_2^a E_3^b | 2a + 3b = k\}$ remains a basis for M_k over $\mathbb{C}$.

It is clear, from the series, that coefficients of the q expansion of both E_2 and E_3 are all integers. Thus, so are coefficients of combinations of E_2 and E_3. Therefore, we have found a basis for M_k such that all elements in the basis have only integer coefficients in their q expansion.

Miller Basis for M_k^0 This is a nice result, but we can in fact do better, by forcing the first coefficients to chosen values.

Theorem 4. *For the space of modular cusp forms M_k^0, there exists a basis $\{f_1, \cdots, f_r\}$ such that:*

- $f_i \in Z[q]$
- $a_i^j = \delta_i j = \begin{cases} 1 & \textit{if } i = j \\ 0 & \textit{if } i \neq j \end{cases} \quad \forall 1 \leq i, j \leq r$
  where a_i^j is the coefficient of q^j in expansion of f_i.

This is commonly called the Miller basis for M_k^0, as it was first introduced by Victor Saul Miller (**?**).

Proof.
- For $k < 6$, $k = 7$, we have $\dim(M_k^0) = 0$. Thus, $\emptyset$ is a basis which satisfies the Miller basis properties.
- For $k = 6$, we have $\dim(M_k^0) = 1$. Thus, $\{\Delta\}$ is a basis which satisfies the Miller basis properties.

- For $k \geq 7$, we let $r = \dim(M_k^0) \geq 1$. We then consider the set

  $$\{g_j | 1 \leq j \leq r\}$$

  where

  $$g_j = \Delta^j E_3^{2(d-j)+b} E_2^a$$

  with

  $$2a + 3b \leq 7 \ \& \ 2a + 3b \cong k \mod 6$$
  $$\& \ \ d = \frac{k - (2a + 3b)}{6} \quad \in \mathbb{N} \text{ as } k \geq 7$$

  Note that a and b are unique unless $k \cong 0 \mod 6$. In witch case, we use by convention $a = 0$, $b = 0$.

  As all E_2, E_3, and Δ have integer coefficients, g_j will as well.

  We then look at the q series:

  $$\Delta(q) = q + O(k^2) \implies \Delta^j(q) = q^j + O(k^{j+1})$$

  As we normalized so,

  $$E_2(q) = 1 + O(q) \implies E_2^\alpha(q) = 1 + O(q)$$
  $$E_3(q) = 1 + O(q) \implies E_3^\alpha(q) = 1 + O(q)$$

  This gives:

  $$g_j(q) = q^j + O(q^{j+1}) \quad \forall 1 \leq j \leq r.$$

  Therefore, $\{g_j, | 1 \leq j \leq r\}$ is clearly a linearly independent set. By dimension argument, it also spans M_k^0. Therefore, it forms a basis. Moreover, in this basis: $a_i^j = \delta_{ij} \quad i \leq j$.

  Finally, we can use Gaussian elimination on $\{g_j\}$ to obtain a basis $\{f_j | 1 \leq j \leq r\}$ such that: $a_i^j = \delta_{ij} \quad \forall 1 \leq i, j \leq r$. The coefficients will remain in $\mathbb{Z}$ after Gaussian elimination.

□

Extension to all M_k We already have a basis for M_k^0, as $\dim(M_k) = \dim(M_k^0) + 1$ (over $\mathbb{C}$), we just need to adjoint one element of $M_k \setminus M_k^0$ to our basis.

It was shown before that $\{E_2^a E_3^b | 2a + 3b = k\}$ is a basis for M_k with integer coefficients (see 2.2.2) One may see from the q expansion that $E_2^a E_3^b = 1 + O(q)$ so $E_2^a E_3^b \in M_k \setminus M_k^0$.

Therefore, we can just add one element of $\{E_2^a E_3^b | 2a + 3b = k\}$ to the Miller basis, and use Gaussian elimination again. We get a basis foe M_k of the form $\{f_j | 0 \leq j \leq r\}$ such that in this basis: $a_i^j = \delta_{ij} \quad \forall 0 \leq i, j \leq r$ (with $r = dim(M_k^0)$ i.e. $r + 1 = dim(M_k)$).

Miller Basis Examples

Miller basis for $k = 16$ We can calculate the Miller basis for $k = 16$: $k \cong 4 \mod 12$ so $a = 2$ and $b = 0$; $d = 2$. We put $g_1 = \Delta^1 E_3^2 E_2^2$, so:

$$\begin{aligned} g_1(q) &= \Delta(q) E_2^2(q) E_3^2(q) \\ &= \left[q - 24q^2 + 252q^3 + O(q^4)\right] \\ &\quad\quad * \left[1 + 240q + 2160q^2 + 6720q^3 + O(q^4)\right]^2 \\ &\quad\quad\quad\quad * \left[1 - 504q - 16632q^2 + 122976q^3 + O(q^4)\right]^2 \\ &= q - 552q^2 - 188244q^3 + O(q^4) \end{aligned}$$

and $g_2 = \Delta^2 E_3^0 E_2^2$, so:

$$\begin{aligned} g_2(q) &= \Delta^2(q) E_2^2(q) \\ &= \left[q - 24q^2 + 252q^3 + O(q^4)\right]^2 \\ &\qquad * \left[1 + 240q + 2160q^2 + 6720q^3 + O(q^4)\right]^2 \\ &= q^2 + 432q^3 + O(q^4) \end{aligned}$$

Then, $f_2 = g_2$ and $f_1 = g_1 + 552g_2$, so:

$$\begin{aligned} f_1(q) &= q - 552q^2 - 188244q^3 + O(q^4) \ + \ 552 * \left[q^2 + 432q^3 + O(q^4)\right] \\ &= q + 50220q^3 + O(q^4) \\ f_2(q) &= q^2 + 432q^3 + O(q^4) \end{aligned}$$

Therefore, up to $O(q^4)$, $\{f_1, f_2\} = \{q + 50220q^3 + O(q^4), q^2 + 432q^3 + O(q^4)\}$ is a basis for M_{16}^0.

To extend this base to M_k, we adjoint a term of the form $g_0 = E_2^a E_3^b$ where $2a + 3b = 16$. We pick $g_0 = E_2^8$, so:

$$\begin{aligned} g_0(q) &= E_2^8(q) \\ &= \left[1 + 240q + 2160q^2 + 6720q^3 + O(q^4)\right]^8 \\ &= 1 + 1920q + 1630080q^2 + 803228160q^3 + O(q^4) \end{aligned}$$

Then, $f_0 = g_0 - 1920g_1 - 1630080g_2$, so:

$$\begin{aligned} f_0(q) &= g_0(q) - 1920g_1(q) - 1630080g_2(q) \\ &= \left[1 + 1920q + 1630080q^2 + 803228160q^3 + O(q^4)\right] \\ &\qquad - 1920\left[q + 50220q^3 + O(q^4)\right] \\ &\qquad\quad - 1630080\left[q^2 + 432q^3 + O(q^4)\right] \\ &= 1 + 2611200q^3 + O(q^4) \end{aligned}$$

Therefore, up to $O(q^4)$, $\{f_0, f_1, f_2\} = \{1+2611200q^3+O(q^4), q+50220q^3+O(q^4), q^2+432q^3+O(q^4)\}$ is a basis for M_{16}.

Miller basis for $k = 92$ The calculation of this basis may be interesting by hand once; However, it is possible to automate it. The procedure that calculates such coefficients is a standard in SageMath(**?**). Here is, up to $O(q^{10})$, the Miller basis for M_{92}:

$$\begin{aligned} f_0 &= 1 + 3034192667130000 * q^8 + 137290127714549760000 * q^9 + O(q^{10}) \\ f_1 &= q + 91578443563200 * q^8 + 2651503140376278561 * q^9 + O(q^{10}) \\ f_2 &= q^2 + 2380310529376 * q^8 + 42238207588515840 * q^9 + O(q^{10}) \\ f_3 &= q^3 + 51682260816 * q^8 + 530253459731160 * q^9 + O(q^{10}) \\ f_4 &= q^4 + 896013480 * q^8 + 4882999541760 * q^9 + O(q^{10}) \\ f_5 &= q^5 + 11516000 * q^8 + 28971735750 * q^9 + O(q^{10}) \\ f_6 &= q^6 + 94680 * q^8 + 80990208 * q^9 + O(q^{10}) \\ f_7 &= q^7 + 312 * q^8 - 4860 * q^9 + O(q^{10}) \end{aligned}$$

2.3 Basis Modulo Two

2.3.1 Reduced Modular Forms

Now that we have a basis with integer coefficients, it makes sense to reduce forms modulo two. For a modular form f, we denote its reduced modulo two from $\overline{f}$. It is defined as follows:

If

$$f(q) = \sum_{n\in\mathbb{N}} c(n)q^n$$

then

$$\overline{f}(q) = \sum_{n\in\mathbb{N}} \overline{c}(n)q^n \qquad \text{with } \; \overline{c}(n) = c(n) \mod 2.$$

We want to reduce Miller basis modulo two. The reason is that as we know that some coefficients are ones, the reduction will not be trivial. We will reduce separately E_2, E_3 and Δ (witch together generate the Miller basis).

E_2 reduced We have:

$$\overline{E_2}(q) = \overline{1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n} = 1 \mod 2$$

Therefore, the reduction modulo two of E_2^a is just 1, for all $a \geq 0$.

E_3 reduced We have:

$$\overline{E_2}(q) = \overline{1 - 504\sum_{n=1}^{\infty}\sigma_5(n)q^n} = 1 \mod 2$$

Therefore, the reduction modulo two of E_3^b is just 1, for all $b \geq 0$ as well.

Δ reduced We defined before Δ, and we would now like to know its q extension in the standard way. That is, an infinite sum of q^n, instead of an infinite product as we have at the moment.

We define the coefficients $\tau(n)$ to match in the equation:

$$\Delta(q) = q\prod_{n=1}^{\infty}(1-q^n)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n$$

When this holds, τ is called the Ramanujan function.

We would like an explicit formula for $\tau(n)$. More precisely, we are interested in a formula for $\tau(n)$ mod 2.

We will calculate separately the coefficients $\tau(n) \mod 2$ for n even and odd.

Case n odd Remember $\sigma_s(n)$ as the sum of s^{th} powers of (positive) divisors of n. It is known from classical theory (**?** , p.8) that:

$$\tau(8n+l) \equiv a_l\sigma_{11}(8n+l) \pmod{2^{b_l}}$$

where $gcd(l,8) = 1$, $a_1 = 1$, $a_3 = 1217$, $a_5 = 1537$, $a_7 = 705$, $b_1 = 11$, $b_3 = 13$, $b_5 = 12$, $b_7 = 14$

We are interested in congruence class (mod 2) of the Ramanujan function $\tau(n)$. For n odd, we deduce the following:

$$\tau(n) \equiv \sigma_{11}(n) \equiv \sum_{d|n} d^{11} \equiv \sum_{d|n} 1 \equiv \begin{cases} 1 \text{ mod } 2 & \text{if } n \text{ is a square} \\ 0 \text{ mod } 2 & \text{else} \end{cases}$$

Case n even It is easy to calculate that $\tau(2) = -24 \equiv 0 \text{ mod } 2$.
Using $\tau(p^{n+1}) = \tau(p^n)\tau(p) - p^{11}\tau(p^{n-1}) \qquad p \in \mathbb{P}$ (**?** , p.97) with $p = 2$, it follows by induction that $\tau(2^k) \equiv 0 \text{ mod } 2 \qquad \forall k \in \mathbb{N}$.
Using $\tau(nm) = \tau(n)\tau(m) \qquad$ if $gcd(n,m) = 1$ (**?** , p.97), it follows that for all n even, $\tau(n) \equiv 0 \text{ mod } 2$.

Explicit series of the discriminant Therefore, the only non-zero coefficients (modulo 2) appears on odd squares, i.e.:

$$\tau(n) \equiv \begin{cases} 1 \bmod 2 & \text{if } n = (2m+1)^2 \quad \text{for } m \in \mathbb{N} \\ 0 \bmod 2 & \text{else} \end{cases}$$

Thus, we can write the power series of Δ as:

$$\Delta(q) \equiv \overline{\Delta}(q) = \sum_{m=0}^{\infty} q^{(2m+1)^2} \mod 2$$

2.3.2 Reduced Basis

The Miller basis for M_k was obtained via the Gauss elimination of the set $\{\Delta^j E_3^{2(d-j)+b} E_2^a | 1 \leq j \leq \dim(M_k)\}$ (with some conditions on a,b,d).

But $\overline{E_2^a} = \overline{E_2}^a = 1^a = 1 \mod 2$ and similarly, $\overline{E_3^{2(d-j)+b}} = 1 \mod 2$. So once the above set is reduced modulo two, we are left with $\{\overline{\Delta}^j | 1 \leq j \leq \dim(M_k)\}$. So the Miller basis just becomes the Gauss elimination of $\overline{\Delta}$ powers.

This is what motivates the next section.

2.4 Space of Modular Forms Modulo Two

We would like to have a definition for this space in a similar way as M_k was used for modular forms (of weight $2k$) before reduction.

2.4.1 Weights of Modular Forms Modulo Two

We just saw that the Miller basis for $\overline{M_k}$ is (the Gaussian elimination of) $\{\overline{\Delta}^j | 1 \leq j \leq \dim(M_k)\}$.

Now, if we look at this set not reduced modulo two, we have: $\{\Delta^j | 1 \leq j \leq \dim(M_k)\}$. This is a set of modular forms that have different weights. However, we started with a modular forms in M_k, i.e. all modular forms having weight $2k$.

We understand now that modulo two, the weight of modular form doesn't make sense any more. This is one of the consequences of reducing modulo two: we lose some informations about the modular forms, such as the weight.

From this observation, we should study all modular forms together, modulo two (instead of separating by weights). This is why the space of modular forms modulo two will be denoted $\mathcal{F}$, with mo dependence on k.

2.4.2 Powers of Δ

Set of Powers of Δ As we just saw, the Gaussian elimination of powers $\overline{\Delta}^k$ up to $\dim(\overline{M_k})$ form the Miller basis of $\overline{M_k}$ (modular forms of weight $2k$ reduced modulo two).

To lighten the notation, we will now write Δ instead of $\overline{\Delta}$, and consider everything modulo two. For simplicity again, we will just take the powers of Δ to be our basis for modular forms modulo two (i.e. drop the Gaussian elimination process).

We define the space $\mathbb{F}_2[\Delta]$ in the usual way:

$$\mathbb{F}_2[\Delta] = \left\{ \sum_{k=1}^{n} a_k \Delta^k | n \in \mathbb{N},\ a_k \in \mathbb{F}_2 \right\}$$

From 2.3.1 we had:

$$\Delta(q) = \sum_{n=0}^{\infty} \tau(n) q^n = \sum_{m=0}^{\infty} q^{(2m+1)^2}$$

Therefore, we define

$$\Delta^k(q) = \sum_{n=0}^{\infty} \tau_k(n) q^n = \left(\sum_{m=0}^{\infty} q^{(2m+1)^2} \right)^k \mod 2$$

Thus, we have $\tau(n) = \tau_1(n)$.

Proportion of zeros In fact, most of the coefficients $\tau_k(n)$ are 0 modulo two.

When $k = 1$, there is already few coefficients that are ones: only the odd squares. When raising to the k^{th} power, there are even "less".

Conditions on non-zero coefficients We can find conditions on coefficients that may not be zero.

We observe: We remark that odd squares are all $1 \mod 8$, and even squares are all $0 \mod 8$.

$a =$	0	1	2	3	4	5	6	7	mod 8
$a^2 =$	0	1	4	1	0	1	4	1	mod 8

Table 1: Squares modulo 8

We know from previous calculations that $\Delta(q)$ only has odd powers of q. Thus, raising to the k^{th} power give terms of power n such that:

$$\begin{aligned} n &= m_1^2 + m_2^2 + m_3^2 + \cdots + m_k^2 \\ &\equiv \ 1 \ + \ 1 \ + \ 1 \ + \cdots + \ 1 \mod 8 \\ &\equiv k \mod 8 \end{aligned}$$

Therefore: $\tau_k(n) \equiv 1 \mod 2 \implies n \equiv k \mod 8$
Equivalently: $n \not\equiv k \mod 8 \implies \tau_k(n) \equiv 0 \mod 2$ (by taking the contra-positive)

This means, that Δ^k may only have terms q^n such that $n \equiv k \mod 8$, i.e. Δ^k may only have terms of power congruent to $k \mod 8$. When $k = 1$, this is that Δ may only have terms of power $1 \mod 8$, this matches with table 1: all odd squares are $1 \mod 8$.

Even powers of Δ We compare $\Delta^{2k}(q)$ and $\Delta^k(q^2)$:

$$\begin{aligned} \Delta^{2k}(q) &= \left(\sum_{m=0}^{\infty} q^{(2m+1)^2} \right)^{2k} \\ &= \sum_{n=0}^{\infty} \#[(2m_1+1)^2 + (2m_2+1)^2 + ... + (2m_{2k}+1)^2 = n \mid m_0, m_1, ..., m_{2k} \in \mathbb{N}] \ q^n \\ &= \sum_{n \ even}^{\infty} \#[(2m_1+1)^2 + (2m_2+1)^2 + ... + (2m_k+1)^2 = n/2 \mid m_0, m_1, ..., m_k \in \mathbb{N}] \ q^n \\ &= \left(\sum_{m=0}^{\infty} q^{((2m+1)^2)*2} \right)^k \\ &= \left(\sum_{m=0}^{\infty} (q^2)^{(2m+1)^2} \right)^k = \Delta^k(q^2) \end{aligned}$$

Thus, $\Delta^{2k}(q) = \Delta^k(q^2)$. Therefore, we can write any modular form modulo two f as the following:

$$f = \sum_{s \geq 0} f_s^{2^s} \quad \text{with } f_s \text{ having only odd powers of } \Delta$$

(**?** , (3)) So it is sufficient to study only the odd powers of Δ.

2.4.3 The Space $\mathcal{F}$

We define the space of modular forms modulo two denoted $\mathcal{F}$ to be(**?** , 2.1):

$$\mathcal{F} = \left\langle \Delta^k | k \text{ odd} \right\rangle = \langle \Delta, \Delta^3, \Delta^5, \Delta^7, \dots \rangle$$

That is, all finite polynomials of Δ over $\mathbb{F}_2$, having only odd powers. We remark that the weight of modular forms do not appear, as it was discussed before in 2.4.1. The observations modulo 8 that we have done in 2.4.2 yields that it will be useful to denote:

$$\mathcal{F}_1 = \left\langle \Delta^k | k = 1 \mod 8 \right\rangle = \langle \Delta, \Delta^9, \Delta^{17}, \Delta^{25}, \cdots \rangle$$

$$\mathcal{F}_3 = \left\langle \Delta^k | k = 3 \mod 8 \right\rangle = \langle \Delta^3, \Delta^{11}, \Delta^{19}, \Delta^{27}, \cdots \rangle$$

$$\mathcal{F}_5 = \left\langle \Delta^k | k = 5 \mod 8 \right\rangle = \langle \Delta^5, \Delta^{13}, \Delta^{21}, \Delta^{29}, \cdots \rangle$$

$$\mathcal{F}_7 = \left\langle \Delta^k | k = 7 \mod 8 \right\rangle = \langle \Delta^7, \Delta^{15}, \Delta^{23}, \Delta^{31}, \cdots \rangle$$

Of course, we have:

$$\mathcal{F} = \mathcal{F}_1 \oplus \mathcal{F}_3 \oplus \mathcal{F}_5 \oplus \mathcal{F}_7$$

We will also introduce (as in (**?** , 2.)):

$$\mathcal{F}(n) = \left\langle \Delta^k | k \text{ odd and } k \leq 2n-1 \right\rangle = \langle \Delta, \Delta^3, \Delta^5, \dots, \Delta^{2n-1} \rangle$$

This matches specifically $\overline{M_{12(2n-1)}} = \mathcal{F}(n)$.

2.4.4 Duality Δ - q

As we defined $\mathcal{F}$ above, a modular form modulo two is an expression of powers Δ^k. But we had from before that $\Delta = \sum_{m=0}^{\infty} q^{(2m+1)^2} \mod 2$. Therefore, we can translate a modular form given as a finite polynomial of Δ into an infinite polynomial of q. Thus, there are two ways to write a modular form modulo two.

This duality between the two definitions is what makes the study of modular forms modulo two so interesting: we go back and forth between an infinite series and a finite polynomial. One is easy to express, the other easy to compute. This will lead to new reasoning. In particular, there is a new technique of computation ("exact computations") that uses equivalence between the two ways of writing a modular form.

2.5 Hecke Operators Modulo Two

2.5.1 Reduction Modulo Two

Definition Now that we have reduced modular forms modulo two, we would like to study the Hecke operators on these reduced modular forms. We define Hecke operators modulo two as follows:

With f a modular form modulo two with q definition

$$f(q) = \sum_{n \in \mathbb{N}} c(n) q^n$$

we define

$$\overline{T_p} | f(q) = \sum_{n \in \mathbb{N}} \gamma(n) q^n$$

where

$$\gamma(n) = \begin{cases} c(np) & \text{if } p \nmid n \\ c(np) + c(n/p) & \text{if } p \mid n \end{cases} \qquad \& \ p \text{ an odd prime}$$

Well-definiteness We want to check that all the definitions make sense. When we look at $T_p|f$, there is a number of ways to to reduce it modulo two: $\overline{T_p|f}$, $\overline{T_p|\overline{f}}$, $\overline{\overline{T_p}|f}$, $\overline{T_p}|\overline{f}$.

Let's compare coefficients:

$\overline{T_p|f}$:

$$\gamma(n) = \sum_{a|(n,p),\, a\geq 1} a^{2k-1} c\left(\frac{np}{a^2}\right) = \begin{cases} \overline{c}(np) & \text{if } p \nmid n \\ \overline{c}(np) + \overline{c}(n/p) & \text{if } p \mid n \end{cases}$$

Divisors of (n,p) are $\{1\}$ or $\{1,p\}$ since p is prime, so the sum split in two cases, with one or two terms. We see now that looking at Hecke operators modulo two only for primes simplifies the sum to a computable formula.

As both 1 and p are odd, the term a^{2k-1} reduces to 1 modulo two. We understand why Hecke operators modulo two isn't defined for even numbers: many terms in the summation would become zero. It would not make sense to call it a Hecke operator any more.

It also makes sense why we look at modular forms modulo two and not say three or five: the coefficient a^{2k-1} collapse nicely modulo two, which won't be the case modulo an other number then two.

$\overline{T_p|\overline{f}}$: This is (very) similar to the case before.

$\overline{T_p}|\overline{f}$:

$$\gamma(n) = \begin{cases} \overline{c}(np) & \text{if } p \nmid n \\ \overline{c}(np) + \overline{c}(n/p) & \text{if } p \mid n \end{cases}$$

$\overline{\overline{T_n}|f}$: Again, this is (very) similar to the case before.

All reductions give in fact the same result, so it makes sense to reduce modular forms modulo two, and still study the Hecke operators (but now only for odd primes). As this all makes sense, we will now write only consider modular forms modulo two, and we will drop the over lines for simplicity.

2.5.2 Properties

What makes Hecke operators interesting, is that they have many properties.

Inherited properties From the fact that $\overline{T_p}|f(q) = \overline{T_p|f(q)}$, we get that the Hecke operators modulo two keep all the properties they had before being reduced.

Modularity Remains From definition 1.7, a Hecke operators transform a modular form to an other. This is because from definition, $T(n)f$ is a sum of modular forms (which remain modular). Therefore, Hecke operators modulo two will as well transform a modular form to an other. This was not clear from the definition modulo two that we had (which was in terms of q series).

Commutativity As in general(**?** , p.101):

$$T(n)T(m) = T(mn) \quad \text{if } \gcd(m,n) = 1$$

We get that:

$$T_pT_q = T_qT_p \quad \forall p,q \in \mathbb{P}$$

Therefore, the Hecke operators modulo two commute. This, as well, was not clear form definition. It will be very convenient for future calculations.

Nilpotent The properties of Hecke operators is that, given a modular form f, if we apply a Hecke operators enough times, the form will become zero (i.e. they are nilpotent).

Order of Δ doesn't increase From definition 1.7, a Hecke operators takes a modular form of weight $2k$ to an other modular form of weight $2k$.

Take a modular form modulo two $\overline{f}$ with degree k (in terms of Δ). Now we want to know the maximum degree (again in terms of Δ) of $T_p|\overline{f}$. Let n be the smallest integer such that $\overline{f} \in \overline{M_{12(2n-1)}}$.

We know $T_p|\overline{f} = \overline{T(p)f}$ and $\overline{f} \in \mathcal{F}(n) = \overline{M_{12(2n-1)}}$ so $f \in M_{12(2n-1)}$. This implies that $T(p)f \in M_{12(2n-1)}$ so $T_p|\overline{f} = \overline{T(p)f} \in \overline{M_{12(2n-1)}} = \mathcal{F}(n)$.

Therefore, the maximum degree (in terms of Δ) of $T_p|\overline{f}$ is k as well. Thus, the degree of $\overline{f}$ doesn't increase after applying a Hecke operator.

Order of Δ decrease (**?** , 2.3) ==> need a proof!!! [I am stuck]

Behaviour of $\mathcal{F}_i$ Suppose $f \in \mathcal{F}_i$, using 2.4.2, we have:

$$f = \sum_{m \equiv i \bmod 8} \mu_m \Delta^m = \sum_{n \equiv i \bmod 8} c(n) q^n$$

From the definition of Hecke operator modulo two (2.5.1), we have:

$$T_p|f = \sum_{n \in \mathbb{N}} \gamma(n) q^n \quad \text{with } \gamma(n) = \begin{cases} c(np) & \text{if } p \nmid n \\ c(np) + c(n/p) & \text{if } p \mid n \end{cases}$$

$c(np)$: We have $np \not\equiv i \mod 8 \implies c(np) = 0$.

$c(n/p)$: As p is an odd prime, it is an odd number, so from 2.4.2, $p^2 \equiv 1 \mod 8$, so $p^{-2} \equiv 1 \mod 8$ as well (with p^{-2} seen mod8).

Therefore, $np \not\equiv i \mod 8 \implies n/p \equiv {}^{np}/_{p^2} \equiv np \not\equiv i \mod 8$.

$\gamma(n)$: We conclude that $n \equiv np^2 \not\equiv pi \mod 8 \implies \gamma(n) = 0$

Using 2.4.2 again, we deduce that $T_p|f \in \mathcal{F}_j$ with $j \equiv pi \mod 8$.

Overall, we have the following:

$$f \in \mathcal{F}_i \implies T_p|f \in \mathcal{F}_j \text{ with } j \equiv pj \mod 8$$

Application to Δ^k As the degree of a modular form doesn't increase after applying a Hecke operator, we can apply this the modular form Δ^k to get:

$$T_p|\Delta^k = \sum_{\substack{j \leq k \\ j \text{ odd}}} \mu_j \Delta^j$$

As we know, moreover, that the degree of a modular form will in fact decrease, we deduce that in fact:

$$T_p|\Delta^k = \sum_{\substack{j \leq k-2 \\ j \text{ odd}}} \mu_j \Delta^j \tag{*}$$

The last observation (on $\mathcal{F}_i$), leads us to the formula:

$$T_p|\Delta^k = \sum_{\substack{j \leq k-2 \\ j \equiv pk \bmod 8}} \mu_j \Delta^j \tag{**}$$

(since $\Delta^k \in \mathcal{F}_i$ with $k \equiv i \mod 8$)

2.5.3 Examples (for Small Powers of Δ)

We will describe the behaviour of Hecke operators when applied to Δ^k with k odd, $k \leq 7$.

Δ Clearly, from (*), we have $T_p|\Delta = 0$, since the sum is empty (for any p odd prime).

Δ^3 From (*), we have $T_p|\Delta^3 = \Delta$ or 0.
Moreover, (**) gives $T_p|\Delta^3 = 0$ if $1 \not\equiv 3p \mod 8$ i.e. if $p \not\equiv 3 \mod 8$.

Now, if $p \equiv 3 \mod 8$, we may only look at the coefficient q^1 of $T_p|\Delta^3$ (if it is 1, $T_p|\Delta^3 = \Delta$ and if it is 0, $T_p|\Delta^3 = 0$, as there is no other possibilities).

From definition (in 2.5.1), we have that the coefficient of q^1 is $\gamma(1) = c(p)$ (since $p \nmid 1$) with c the q coefficients of Δ^3.

From (2.3.1), the none zero coefficients of Δ are odd squares.

Now, $c(p)$ is th p^{th} coefficient of Δ^3. We have:

$$(\Delta(q))^3 = \left(\sum_{m=0}^{\infty} q^{(2m+1)^2}\right)^3 = \sum_{n=0}^{\infty} \#\{m_1, m_2, m_3 \text{ odds } | m_1^2 + m_2^2 + m_3^2 = n\} q^n$$

So $c(p) = \#\{m_1, m_2, m_3 \text{ odds } | m_1^2 + m_2^2 + m_3^2 = p\} \mod 2$ corresponds $(\bmod 2)$ to the number of ways to write p as sum of three odd squares.

Need in fact $m_1 = m_2 \neq m_3$, but then?? [I am stuck]

Δ^5 From (*), we have $T_p|\Delta^5 = \Delta^3$ or Δ or 0.
Moreover, (**) gives:

$$\begin{array}{rlccc} p \equiv 7 \bmod 8: & T_p|\Delta^5 = \Delta^3 \text{ or } 0 & \text{if } 3 \equiv 5p \mod 8 & \text{i.e. } p \equiv 7 \mod 8 \\ p \equiv 5 \bmod 8: & T_p|\Delta^5 = \Delta \text{ or } 0 & \text{if } 1 \equiv 5p \mod 8 & \text{i.e. } p \equiv 5 \mod 8 \\ p \equiv 1 \text{ or } 3 \bmod 8: & T_p|\Delta^5 = 0 & \text{else} & \end{array}$$

Now, if $p \equiv 7 \mod 8$, we may only look at the coefficient q^3 of $T_p|\Delta^5$ (if it is 1, $T_p|\Delta^5 = \Delta^3$ and if it is 0, $T_p|\Delta^3 = 0$, as there is no other possibilities).

From definition (in 2.5.1), we have that the coefficient of q^3 is $\gamma(3) = c(3p)$ (since $p \nmid 3$) with c the q coefficients of Δ^5.

From (2.3.1), the none zero coefficients of Δ are odd squares. Now, $c(3p)$ is th p^{th} coefficient of Δ^5. We have:

$$(\Delta(q))^5 = \left(\sum_{m=0}^{\infty} q^{(2m+1)^2}\right)^5 = \sum_{n=0}^{\infty} \#\{m_1, m_2, m_3, m_4, m_5 \text{ odds } | m_1^2 + m_2^2 + m_3^2 + m_4^2 + m_5^2 = n\} q^n$$

So $c(3p) = \#\{m_1, m_2, m_3, m_4, m_5 \text{ odds } | m_1^2 + m_2^2 + m_3^2 + m_4^2 + m_5^2 = 3p\} \mod 2$ corresponds $(\bmod 2)$ to the number of ways to write $3p$ as sum of five odd squares.

When looked $\bmod 8$, $m_1^2 + m_2^2 + m_3^2 + m_4^2 + m_5^2 \equiv 5 \mod 8$. We can check, $p \equiv 7 \mod 8$ so $3p \equiv 5 \mod 8$.

Need in fact $m_1 = m_2 \neq m_3$, but then?? [I am stuck]

Δ^7

2.5.4 Nilpotent Order

As we know that the Hecke operators are nilpotent, we may want to study the order of nil potentness.

Definition

Properties

Example We will look at Δ^{95}...

3 Class Field Theory

3.1 Context

Let R be a commutative ring, M and P ideals in R. We can then prove the followings:

Theorem 5. • *M is maximal $\iff$ R/M is a field*

- *P is prime $\iff$ R/P is an integral domain*

Property 3.1. *Maximal ideals are prime.*

Proof.

$$\begin{aligned} M \text{ maximal ideal} &\iff R/M \text{ field} \\ &\implies \text{R/M Integral Domain} \iff M \text{ prime ideal} \end{aligned}$$

□

If L/K is a Galois extension, then we will denote it's Galois group by $\mathrm{Gal}(L/K)$.

———

Let K be a number field, and $\mathcal{O}_K$ be the corresponding ring of integers. Let $\mathfrak{p}$ be a non-zero prime ideal in $\mathcal{O}_K$. Let L/K be a finite extension and again, $\mathcal{O}_L$ be the ring of integers in L.

Then we know that $\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ in L

We have $\mathfrak{p}\mathcal{O}_L$ an ideal in $\mathcal{O}_L$. It is not a prime ideal in general, but as L/K is finite, there exists a factorization as the following:

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$$

Where the integers e_i are called the ramification indexes. We also have $\mathfrak{P}_i \cap \mathcal{O}_K = \mathfrak{p}$, and we say that the ideals $\mathfrak{P}_i$ in L extend the ideal $\mathfrak{p}$ in K.

Then, there are three possibilities for an ideal: it may split, ramifies of be inert.

Definition 3.1 (Ideal Ramifies). *We say that an ideal $\mathfrak{p}$ ramifies in L/K if a ramification index e_i is greater then one, i.e. if $e_i > 1$ for some $1 \leq i \leq r$.*

Definition 3.2 (Ideal Splits). *We say that $\mathfrak{p}$ splits in L/K if none of the ramification indexes e_i is greater then one, and r is a least two; i.e. if $e_i = 1 \quad \forall 1 \leq i \leq r$ and $r \geq 2$.*

Definition 3.3 (Ideal Inert). *We say that $\mathfrak{p}$ is inert in L/K if there is only one ramification index e_1 and it is equal to one; i.e. if $e_1 = 1$ and $r = 1$.*

We know that the extension L/K is ramified in the primes that divide the discriminant. Therefore, the extension is unramified in all but finitely many prime ideals.

3.2 Residue Fields Extensions

The ideal $\mathfrak{p}$ defines the residue field $F = \mathcal{O}_K/\mathfrak{p}$. The ideals $\mathfrak{P}_i$ define the residue fields $F_i = \mathcal{O}_L/\mathfrak{P}_i$. The field F then naturally embeds to F_i (so each $\mathfrak{P}_i$ defines a field extension). The inertia degree of $\mathfrak{P}_i$ is the degree $f_i = [F_i : F] = [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$ of this extension.

We then observe that $[L : K] = \sum_{i=1}^{r} e_i f_i$

We can then specify when an ideal splits or ramifies completely.

Definition 3.4 (Ideal Splits Completely). *We say that $\mathfrak{p}$ splits completely in L/K if all ramification indexes e_i and inertia degrees f_i are one. i.e. if $e_i = f_i = 1 \quad \forall 1 \leq i \leq r$.*
In this case, $r = [L : K]$.

Definition 3.5 (Ideal Ramifies Completely). *We say that $\mathfrak{p}$ ramifies completely in L/K if the inertia degrees f_1 is one, and r is one. i.e. if $r = 1$ and $f_1 = 1$.*
In this case, $e_1 = [L : K]$.

3.3 Norms of Ideals

We define the norm of an ideal I in $\mathcal{O}_K$ as $N(I) = |\mathcal{O}_K/I|$.

If $\mathfrak{p} \subset \mathcal{O}_K$ is a prime ideal, then we can put $(p) = \mathfrak{p} \cap \mathbb{Z}$. It follows that $p\mathcal{O}_K \subset \mathfrak{p}$. $\mathcal{O}_K$ is a free $\mathbb{Z} - module$ of rank $[K : \mathbb{Q}] = q$, i.e. $\exists \alpha_1, \dots, \alpha_q$ s.t. $\mathcal{O}_K = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_q$. Thus, $|\mathcal{O}_K/\mathfrak{p}| \leq |\mathcal{O}_K/(p)| \leq p^q$.

We have $Norm(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}| = p^m$ and $Norm_{L/\mathbb{Q}}(\mathfrak{P}_i) = Norm_{K/\mathbb{Q}}(\mathfrak{p})^{f_i}$. This implies $Norm(\mathfrak{P}_i) = |\mathcal{O}_L/\mathfrak{P}_i| = p^{mf_i}$.
We also have: $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_{Norm(\mathfrak{p})}$ and $\mathcal{O}_L/\mathfrak{P}_i \cong \mathbb{F}_{Norm(\mathfrak{P}_i)}$

3.4 Galois Extensions Simplifications

When the extension L/K is Galois, the ramification indexes e_i are all the same ($e_i = e$), as well as the inertia degrees $f_i = f$. We then have

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{r} \mathfrak{P}_i^e \text{ and } [L : K] = ref$$

The Galois group Gal(L/K) is often denoted G

We define the decomposition group $G_{\mathfrak{P}}$ of the ideal $\mathfrak{P}$ to be $\{\sigma \in G | \sigma(\mathfrak{P}) = \mathfrak{P}\}$. It turns out that $G_{\mathfrak{P}} \cong \text{Gal}({}^{\mathcal{O}_L/\mathfrak{P}}/{}_{\mathcal{O}_K/\mathfrak{p}}) \cong \text{Gal}(\mathbb{F}_{p^{mf}}/\mathbb{F}_{p^f})$. Moreover, it is a cyclic group, so $G_{\mathfrak{P}} =< \tilde{\sigma} >$.

3.5 Unramified Prime Simplifications

When the ideal $\mathfrak{p}$ is unramified, $e = 1$, so we get:

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{r} \mathfrak{P} \text{ and } [L : K] = rf$$

3.6 The Frobenius Element

3.6.1 Definition

[is it ok a a subsection title? (perhaps too generic?) alternatives: well definiteness, introduction,]

We can construct the Frobenius element (sometimes also called the Artin symbol, or the Frobenius map) that depend on the extension L/K and ideal $\mathfrak{P}$ in $\mathcal{O}_L$. It is denoted Frob$_{L/K}(\mathfrak{P})$, and is *the* element $\sigma \in G$ such that:

$$\sigma(\alpha) \equiv \alpha^{Norm(\mathfrak{p})} \bmod \mathfrak{P} \quad \forall \alpha \in \mathcal{O}_L.$$

At the moment, we can not talk of the Frobenius element as it is not unique: it is unique only up to a conjugacy class. This is not too pathological, as Frobenius element of primes ideals $\mathfrak{P}_1$ and $\mathfrak{P}_2$ that extend the same prime $\mathfrak{p}$ are conjugates.

We define the Frobenius element for $\mathfrak{p}$ (denoted Frob$_{L/K}(\mathfrak{p})$) in a meaning full manner, to be the set $\{\text{Frob}_{L/K}(\mathfrak{P}) | \mathfrak{P} \text{ extending } \mathfrak{p}\} \subset G$.

[is this construction / definition ok? or maybe I should rephrase it? (it look weird to me)]

Property 3.2. *If $\tau \in G$, then Frob$_{L/K}(\tau\mathfrak{P}) = \tau$Frob$_{L/K}(\mathfrak{P})\tau^{-1}$.*

Proof. For all $x \in \mathcal{O}_L$, we have:

$$\text{Frob}_{L/K}(\mathfrak{P})x = x^{Norm(\mathfrak{p})} \mod \mathfrak{P}$$

But all such x may be written as $\tau^{-1}(x)$, so we have:

$$\text{Frob}_{L/K}(\mathfrak{P})\tau^{-1}(x) = (\tau^{-1}x)^{Norm(\mathfrak{p})} \mod \mathfrak{P}$$

Which gives:

$$\tau\text{Frob}_{L/K}(\mathfrak{P})\tau^{-1}(x) = x^{Norm(\mathfrak{p})} \mod \mathfrak{P}$$

□

Property 3.3. *If $\mathfrak{P}_1$ and $\mathfrak{P}_2$ extend $\mathfrak{p}$, then $Frob_{L/K}(\mathfrak{P}_1)$ and $Frob_{L/K}(\mathfrak{P}_2)$ are conjugates.*

Proof. We have the following scheme:

$$\begin{tikzcd}
L \arrow[d, dash] & \supseteq & \mathfrak{P}_1 \arrow[d, dash] & \mathfrak{P}_2 \arrow[dl, dash] \\
K & \supseteq & \mathfrak{p} &
\end{tikzcd}$$

There is an element $\tau \in G$ such that $\tau(\mathfrak{P}_1) = \mathfrak{P}_2$. Then using last property, we deduce that $\text{Frob}_{L/K}(\mathfrak{P}_1)$ and $\text{Frob}_{L/K}(\mathfrak{P}_2)$ are conjugates. □

Never the less, is important to notice at this point that if G is abelian, then all conjugacy classes are made up of only one element. Therefore, the Frobenius element is well defined in this case. Moreover, it will only depend on the prime $\mathfrak{p}$ that is extended. [should this comment be before or after the property?]

3.6.2 Examples

Case $\mathbb{Q}[\sqrt{7}] : \mathbb{Q}$ (quadratic field extension) We have minimum polynomial $m(x) = x^2 - 7$, the discriminant is $\Delta = 4.7 = 28$.
We write $G = \text{Gal}(\mathbb{Q}[\sqrt{7}] : \mathbb{Q}) =< \sigma \mid \sigma^2 = 1_G > \cong C_2$.

The prime ideal (2) As $m(x) = (x+1)^2 \mod 2$, we have $(2) = (2, \sqrt{7}+1)^2$.
As well, $Norm((2)) = 2^2 = 4$ and $Norm((2, \sqrt{7}+1)) = 2$.

So we have:

$$\begin{aligned} \text{Frob}_{\mathbb{Q}[\sqrt{7}]:\mathbb{Q}}((2, \sqrt{7}+1)) : \alpha &\to \alpha^{Norm((2))} \ (3, \sqrt{7}+1) \\ \sqrt{7} &\to [\sqrt{7}]^4 \ (2, \sqrt{7}+1) = -\sqrt{7} \ (2, \sqrt{7}+1) \end{aligned}$$

Thus, $\text{Frob}_{\mathbb{Q}[\sqrt{7}]:\mathbb{Q}}((2, \sqrt{7}+1)) = \sigma \in G$.

The prime ideal (3) As $m(x) = (x+1)(x-1) \mod 3$, we have $(3) = (3, \sqrt{7}+1)(3, \sqrt{7}-1)$.
As well, $Norm((3)) = 3^2 = 9$ and $Norm((3, \sqrt{7}+1)) = Norm((3, \sqrt{7}-1)) = 3$.

So we have:

$$\begin{aligned} \text{Frob}_{\mathbb{Q}[\sqrt{7}]:\mathbb{Q}}((3, \sqrt{7}+1)) : \alpha &\to \alpha^{Norm((3))} \ (3, \sqrt{7}+1) \\ \sqrt{7} &\to [\sqrt{7}]^9 \ (3, \sqrt{7}+1) = \sqrt{7} \ (3, \sqrt{7}+1) \end{aligned}$$

Thus, $\text{Frob}_{\mathbb{Q}[\sqrt{7}]:\mathbb{Q}}((3, \sqrt{7}+1)) = 1_G \in G$. Similarly, $\text{Frob}_{\mathbb{Q}[\sqrt{7}]:\mathbb{Q}}((3, \sqrt{7}-1)) = 1_G \in G$.

Case $\mathbb{Q}[\zeta_6] : \mathbb{Q}$ (6^{th} cyclotomic field extension) We have minimum polynomial $m(x) = x^2 - x + 1$ (so the degree of the extension is 2), the discriminant is $\Delta = -3$ (here, $\zeta_6 = e^{\pi i/3}$ denotes the 6^{th} root of unity).

We write $G = \text{Gal}(\mathbb{Q}[\zeta_6] : \mathbb{Q}) =< \sigma : \zeta_6 \to \zeta_6^2, \tau : \zeta_6 \to \zeta_6^3 \mid \sigma^3 = \tau^2 = Id, \sigma\tau = \tau\sigma > \cong C_2 \times C_3$. Note that $g \in G$ is determined by $g(\zeta_6)$. Note as well that G is abelian, so the Frobenius element is well defined.

The prime ideal (3) As $m(x) = (x+1)^2 \mod 3$, we have $(3) = (3, \zeta_6 + 1)^2$.
As well, $Norm((3)) = 3^2 = 9$ and $Norm((3, \zeta_6+1)) = Norm((3, \zeta_6 - 1)) = 3$.

So we have:

$$\begin{aligned} \text{Frob}_{\mathbb{Q}[\zeta_6]:\mathbb{Q}}((3, \zeta_6+1)) : \alpha &\to \alpha^{Norm((3))} \ (3, \zeta_6+1) \\ \zeta_6 &\to [\zeta_6]^9 \ (3, \zeta_6+1) = -1 \ (3, \zeta_6+1) = \zeta_6 \ (3, \zeta_6+1) \end{aligned}$$

Thus, $\text{Frob}_{\mathbb{Q}[\zeta_6]:\mathbb{Q}}((3, \zeta_6+1)) = Id \in G$.

The prime ideal (7) As $m(x) = (x+2)(x-3) \mod 3$, we have $(7) = (7, \zeta_6 + 2)(7, \zeta_6 - 3)$. As well, $Norm((7)) = 7^2 = 49$ and $Norm((7, \zeta_6 + 2)) = Norm((3, \zeta_6 - 3)) = 7$.

So we have:

$$\begin{aligned} \mathrm{Frob}_{\mathbb{Q}[\zeta_6]:\mathbb{Q}}((7, \zeta_6 + 2)) : \alpha &\to \alpha^{Norm((7))} \ (7, \zeta_6 + 2) \\ \zeta_6 &\to [\zeta_6]^49 \ (7, \zeta_6 + 2) = \zeta_6 \ (7, \zeta_6 + 2) \end{aligned}$$

Thus, $\mathrm{Frob}_{\mathbb{Q}[\zeta_6]:\mathbb{Q}}((7, \zeta_6 + 2)) = Id \in G$. Similarly, $\mathrm{Frob}_{\mathbb{Q}[\zeta_6]:\mathbb{Q}}((7, \zeta_6 - 3)) = Id \in G$.

The prime ideal (13) As $m(x) = (x+3)(x-4) \mod 3$, we have $(13) = (13, \zeta_6 + 3)(13, \zeta_6 - 4)$. As well, $Norm((13)) = 13^2 = 169$ and $Norm((13, \zeta_6 + 3)) = Norm((3, \zeta_6 - 4)) = 13$.

So we have:

$$\begin{aligned} \mathrm{Frob}_{\mathbb{Q}[\zeta_6]:\mathbb{Q}}((13, \zeta_6 + 3)) : \alpha &\to \alpha^{Norm((13))} \ (13, \zeta_6 + 3) \\ \zeta_6 &\to [\zeta_6]^169 \ (13, \zeta_6 + 3) = \zeta_6 \ (13, \zeta_6 + 3) \end{aligned}$$

Thus, $\mathrm{Frob}_{\mathbb{Q}[\zeta_6]:\mathbb{Q}}((13, \zeta_6 + 3)) = Id \in G$. ?? always identity?? [to be solved]

3.6.3 Behaviour in Chained Extensions

We will consider the following scheme:

$$\begin{tikzcd} \mathcal{O}_M \subset M \arrow[d, dash] & \supseteq & \mathfrak{P} \arrow[d, dash] \\ \mathcal{O}_L \subset L \arrow[d, dash] & \supseteq & \mathfrak{p} \arrow[d, dash] \\ \mathcal{O}_K \subset K & \supseteq & p \end{tikzcd}$$

In such a situation, we can define (for M/K Galois) $\mathrm{Frob}_{M/K}(\mathfrak{P})$, $\mathrm{Frob}_{M/K}(p)$, $\mathrm{Frob}_{M/L}(\mathfrak{P})$, $\mathrm{Frob}_{M/L}(\mathfrak{p})$. If, in addition, L/K is normal: $\mathrm{Frob}_{L/K}(\mathfrak{p})$, and $\mathrm{Frob}_{L/K}(p)$. (**?** , p.99)

We will look at properties of these Frobenius elements (relation between each others).

Property 3.4.

$$Frob_{M/K}(\mathfrak{P})^{f(\mathfrak{P}/\mathfrak{p})} = Frob_{M/L}(\mathfrak{P})$$

[what is this $f(\mathfrak{P}/\mathfrak{p})$? is it the fields of $\mathfrak{P}$ over $\mathfrak{p}$?]

to write... (**?** , p.99) □

Property 3.5.

$$Frob_{L/K}(\mathfrak{p}) = Frob_{M/K}(\mathfrak{P})\big|_L$$

Proof. Let $\sigma = \mathrm{Frob}_{M/K}(\mathfrak{P}) \in \mathrm{Gal}(M/K)$ so $\sigma : M \to M$ s.t. $\sigma|_K = Id$ and σ is an autotomorphism. Similarly, let $\tau = \mathrm{Frob}_{L/K}(\mathfrak{p}) \in \mathrm{Gal}(L/K)$ so $\tau : L \to L$ s.t. $\tau|_K = Id$ and τ is an autotomorphism.

As M extends L, σ being an automorphism of M makes it an automorphism of L as well. The restriction condition stays the same. □

Property 3.6.

$$Gal(L/K) \cong {}^{Gal(M/K)}/_{Gal(M/L)}$$

Proof. Let $\sigma \in \mathrm{Gal}(M/K)$, i.e. $\sigma : M \to M$ s.t. $\sigma|_K = Id$ and σ is an autotomorphism.

Let $\phi : \mathrm{Gal}(M/K) \to \mathrm{Gal}(L/K)$ be such that: $\phi(\sigma) = \sigma|_L$. This is well defined as an automorphism of M restricts to an automorphism of L when M extends L.

It is trivial to check that ϕ is a homomorphism.

The kernel of ϕ is clearly $\mathrm{Gal}(M/L)$.

The image of ϕ is $\mathrm{Gal}(L/K)$ as every element of $\mathrm{Gal}(L/K)$ may be extended to $\mathrm{Gal}(M/K)$.

Therefore, the property follows via the 1^{st} isomorphism theorem. □

Property 3.7. *We have:*

$$\mathfrak{p} \textit{ splits complitely in } L \iff \mathit{Frob}_{L/K}(\mathfrak{P}) = 1$$

(**?** , p.100)

We will consider the following scheme:

$$\begin{tikzcd}
 & L_1L_2 \supseteq \mathfrak{P} \arrow[dl, no head] \arrow[dr, no head] & \\
L_1 \supseteq \mathfrak{p}_1 \arrow[dr, no head] & & L_2 \supseteq \mathfrak{p}_2 \arrow[dl, no head] \\
 & K \supseteq \mathfrak{p} &
\end{tikzcd}$$

Property 3.8. *We have:*

$$\mathit{Frob}_{L_1L_2/K}(\mathfrak{P}) = \mathit{Frob}_{L_1/K}(\mathfrak{p}_1) \times \mathit{Frob}_{L_2/K}(\mathfrak{p}_2)$$

(**?** , p.100)

Property 3.9. *We have:*

$$\mathfrak{p} \textit{ splits complitely in } L_1L_2 \iff \mathfrak{p} \textit{ splits complitely in } L_1 \textit{ and } L_2$$

Proof. Combine the last two proposition. (**?** , p.100) □

3.7 The Chebotarev's Density Theorem

3.7.1 Motivations

If we look at the distribution of primes numbers modulo a number (15 in the next example), we get a table as follows:

Table mod 15:
0:
1: 31, 61, 151, 181, 211, 241, 271, 331, 421,
2: 2, 17, 47, 107, 137, 167, 197, 227, 257, 317, 347, 467,
3: 3,
4: 19, 79, 109, 139, 199, 229, 349, 379, 409, 439, 499,
5: 5,
6:
7: 7, 37, 67, 97, 127, 157, 277, 307, 337, 367, 397, 457, 487,
8: 23, 53, 83, 113, 173, 233, 263, 293, 353, 383, 443,
9:
10:
11: 11, 41, 71, 101, 131, 191, 251, 281, 311, 401, 431, 461, 491,
12:
13: 13, 43, 73, 103, 163, 193, 223, 283, 313, 373, 433, 463,
14: 29, 59, 89, 149, 179, 239, 269, 359, 389, 419, 449, 479,

It looks like there are classes of primes. We would like to characterize this repartition: that is, decide if classes are finite or infinite, and quantify the repartitions.

3.7.2 Notions of Density

As discussed previously, we are interested in subsets of $\mathbb{P}$ (the set of primes numbers). Euler proved that there are infinitely many primes. Therefore, there are two types of subsets of $\mathbb{P}$: the ones that are infinite, and the finites ones. For finite sets, we can characterise the size by just counting elements. In fact, we will mainly be interested in sets that have infinitely many primes, and again, we would like a notion of size.

A suitable way would be to compare the subset with the set of all primes, and, say look at the proportions of primes included in the subset.

We call this the density, there are two rigorous ways to define it:

Definition 3.6 (Natural density). *We say that $S \subseteq \mathbb{P}$ has natural density δ when:*

$$\lim_{x \to +\infty} \frac{\#\{p \in \mathbb{P} | p \in S\}}{\#\{p \in \mathbb{P} | p \in \mathbb{P}\}} = \delta$$

Definition 3.7 (Analytic density or Dirichlet density). *We say that $S \subseteq \mathbb{P}$ has analytical (or Dirichlet) density δ when:*

$$\lim_{s \to 1^+} \left(\sum_{p \in S} \frac{1}{p^s} \right) \left(\sum_{p \in \mathbb{P}} \frac{1}{p} \right)^{-1} = \delta$$

Note that the natural density may not exist. However, when both exist, the two densities are the same.

3.7.3 Theorem

One of the most important results that use Frobenian maps is probably the Chebotarev density theorem.

Theorem 6. *With L/K an extension of Galois group $G = Gal(L/K)$.*
Let C be a conjugacy class in G.

Then, the proportion of unramified primes ideals $\mathfrak{p}$ in K that have Frobenius element $Frob_{L/K}(\mathfrak{p}) = C$ [2] *is $|C|/|G|$.*

We see that Frobenius elements are in the heart of this theorem.

Proof [quick proof? actually, I couldn't find one, maybe just idea of proof?]

Example Extension with non-commutative Galois group (as commutative will be used in Dirichlet's example). => splitting field of $x^3 - 2$? (i.e. $\mathbb{Q}[\zeta_3, \sqrt[3]{2}] : \mathbb{Q}$)

3.8 The Dirichlet's Density Theorem

3.8.1 Theorem

The most common application of Chebotarev density theorem is probably the Dirichlet's density theorem. It states as follows:

Theorem 7. *Let $n \in \mathbb{N}^*$, $a \in \mathbb{N}$ such that $\gcd(a, n) = 1$. If $S = \{p \in \mathbb{P} | p \equiv a \mod n\}$, then S has density $1/\varphi(n)$.*

[2] When depending on a prime in the "lower" field, the Frobenius element is a conjugacy class to be well defined

3.8.2 Link with Chebotarev

This is a direct application of Chebotarev's density theorem for the field extension $\mathbb{Q}[\gamma] : \mathbb{Q}$ where γ is the n^{th} root of unity (this is the cyclotomic field).

The Galois group then is cyclic, as this is a cyclotomic extension, and has order $\varphi(n)$ by definition (so $\mathrm{Gal}(\mathbb{Q}[\gamma] : \mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z}) \cong C_{\varphi(n)}$).

Primes ideals in $\mathbb{Q}$ are just primes numbers. And as the Galois group is cyclic, it is abelian, so all conjugacy classes have one element. Thus, Chebotarev gives Dirichlet's density theorem in the particular case of cyclotomic extensions.

3.8.3 Proof

[Stand alone proof?]

3.8.4 Example

[Prove the case n=15 from the motivation subsection above.]

References