Student seminar notes week 6

Marilou Bezos after the talk of Beatrice Pedroni and Junda Long

1 Dirichlet Density

Definition 1.1. Let $f, g : (1; \infty) \to \mathbb{R}$ defined for $s \in \mathbb{R}, s > 1$. We write $f \sim g$ when $f(s) - g(s)$ is bounded as $s \to 1^+$.

Remark 1.2 (reformulation of Dirichlet's Theorem)**.** We take a and m as in Dirichlet's Theorem on primes in arithmetic progressions, i.e., m a positive integer and a such that $(a, m) = 1$.
Recall that for any χ Dirichlet character, we have

$$\begin{aligned}\log L(s,\chi) &= \sum_{p \text{ prime}} \frac{\chi(p)}{p^s} + \{ \text{ Dirichlet series converging for } \mathrm{Re}(s) > 1/2\} \\ &\sim \sum_{p \text{ prime}} \frac{\chi(p)}{p^s}.\end{aligned}$$

We assume that $L(1, \chi) \neq 0$ if $\chi \neq \chi_0$ thus we have

$$\begin{aligned}\sum_{\chi \in \widehat{(\mathbb{Z}/m\mathbb{Z})^\times}} \chi(a)^{-1} \log L(s,\chi) &\sim \sum_{\chi} \chi(a)^{-1} \sum_{p \text{ prime}} \frac{\chi(p)}{p^s} \\ &\sim \sum_{p \equiv a \bmod m} \frac{\varphi(m)}{p^s} \sim \log L(s, \chi_0).\end{aligned}$$

Now

$$L(s,\chi_0) = \prod_p \left(1 - \frac{\chi_0(p)}{p^s}\right)^{-1} = \left(\prod_{p|m} (1 - p^{-s})\right) \zeta(s),$$

so $\log L(s, \chi_0) \sim \log \zeta(s)$ and

$$\underbrace{\sum_{p \equiv a \bmod m} \frac{1}{p^s}}_{\text{diverges as } s \to 1^+} \sim \frac{1}{\varphi(m)} \log \zeta(s). \tag{1}$$

Since ζ has a pole in $s = 1$ we have that $\log \zeta(s) \xrightarrow{s \to 1^+} \infty$, the sum cannot consist of only finitely many terms, and this gives us Dirichlet's Theorem.

Now that we have reformulated the Theorem, this leads us to the new notion of Dirichlet density. Note that

$$\begin{aligned}\frac{1}{\varphi(m)}\log\zeta(s) =& \frac{1}{\varphi(m)}\left(\underbrace{\log((s-1)\zeta(s))}_{\xrightarrow{s\to 1^+}1} + \log\left(\frac{1}{s-1}\right)\right)\\ \sim& \frac{1}{\varphi(m)}\log\left(\frac{1}{s-1}\right).\end{aligned}$$

Hence using (1) we have

$$\sum_{p\equiv a \bmod m} p^{-s} \sim \frac{1}{\varphi(m)}\log\left(\frac{1}{s-1}\right).$$

If we reformulate this means that

$$\lim_{s\to 1^+}\frac{\sum_{p\equiv a \bmod m} p^{-s}}{\log\left(\frac{1}{s-1}\right)} = \frac{1}{\varphi(m)}.$$

This motivates the following definition:

Definition 1.3 (Dirichlet density)**.** Let $\mathcal{S}$ be any set of primes. If

$$\lim_{s\to 1^+}\frac{\sum_{p\in\mathcal{S}} p^{-s}}{\log(\frac{1}{s-1})} = \delta \text{ exists.}$$

Then we say that $\mathcal{S}$ has Dirichlet density $\delta = \delta(\mathcal{S})$.

Example 1.4 (Dirichlet Theorem)**.** If $\mathcal{S} = \{\text{primes } p : p \equiv a \bmod m\}$ then $\delta(\mathcal{S}) = \frac{1}{\varphi(m)}$.

Lemma 1.5. *Suppose $\mathcal{S}$ and $\mathcal{T}$ are sets of primes such that $\mathcal{S}\cap\mathcal{T} = \emptyset$, then if any two of $\delta(\mathcal{S}), \delta(\mathcal{T})$ or $\delta(\mathcal{S}\cup\mathcal{T})$ are finite then so is the third, and in that case we have*

$$\delta(\mathcal{S}\cup\mathcal{T}) = \delta(\mathcal{S}) + \delta(\mathcal{T}).$$

Proof. Since we assume that $\mathcal{S}\cap\mathcal{T} = \emptyset$, using the definition of the density we have:

$$\begin{aligned}\lim_{s\to 1^+}\frac{\sum_{p\in(\mathcal{S}\cup\mathcal{T})} p^{-s}}{\log(\frac{1}{s-1})} &\underbrace{=}_{\mathcal{S}\cap\mathcal{T}=\emptyset} \lim_{s\to 1^+}\frac{\sum_{p\in\mathcal{S}} p^{-s} + \sum_{p\in\mathcal{T}} p^{-s}}{\log(\frac{1}{s-1})}\\ &= \lim_{s\to 1^+}\frac{\sum_{p\in\mathcal{S}} p^{-s}}{\log(\frac{1}{s-1})} + \lim_{s\to 1^+}\frac{\sum_{p\in\mathcal{T}} p^{-s}}{\log(\frac{1}{s-1})}.\end{aligned}$$

Thus, if any two of the three limits exists, the third one exists and we get the equality that we wanted. □

Theorem 1.6. *Let $K/\mathbb{Q}$ be Galois, and let*

$$\mathcal{S}_K = \{p \in \mathbb{Z} : p \text{ splits completely in } K/\mathbb{Q}\}.$$

Then $\delta(\mathcal{S}_K) = 1/[K:\mathbb{Q}]$.

Proof. Let $\zeta_K(s) = \prod_{\mathfrak{p}\subset\mathcal{O}_K \text{ prime}}(1 - N_{\mathfrak{p}}^{-s})^{-1}$ for $\mathrm{Re}(s) > 1$, be the Dedekind zeta function for K. We have for $s \in \mathbb{R}, s > 1$:

$$\begin{aligned}\log\zeta_K(s) =& -\sum_{\mathfrak{p}\subset\mathcal{O}_K \text{ prime}} \underbrace{\log(1 - N_{\mathfrak{p}^{-s}})}_{\text{well defined: } 1/N_{\mathfrak{p}}<1}\\ =&\sum_{\mathfrak{p}}\sum_{n=1}^{\infty}\frac{1}{n}N_{\mathfrak{p}}^{-ns} \sim \sum_{\mathfrak{p}} N_{\mathfrak{p}}^{-s} + \underbrace{\sum_{\mathfrak{p}}\sum_{n=2}^{\infty}\frac{1}{n}N_{\mathfrak{p}}^{-ns}}_{(\bullet)\text{ bounded as } s\to 1^+}\\ \sim&\sum_{\mathfrak{p}} N_{\mathfrak{p}}^{-s}.\end{aligned}$$

Let us show $(\bullet)$:

$$\begin{aligned}\sum_{n=2}^{\infty}\frac{1}{n}N_{\mathfrak{p}}^{-ns} \leq& \frac{N_{\mathfrak{p}}^{-2s}}{1 - N_{\mathfrak{p}}^{-s}}\\ \leq& 2N_{\mathfrak{p}}^{-2s}.\end{aligned}$$

Thus we have

$$\sum_{\mathfrak{p}}\sum_{n=2}^{\infty}\frac{1}{n}N_{\mathfrak{p}}^{-ns} \leq \sum_{\alpha\subset\mathcal{O}_K \text{ ideal}} 2N_{\alpha}^{-2s} = 2\zeta_K(2s) \underbrace{<}_{2s>2>1} \infty.$$

Now see that $\log\zeta_K(s) = \log((s-1)(\zeta_K(s)) + \log(1/(s-1)) \sim \log(1/(s-1))$,thus we have

$$\begin{aligned}\log\zeta_K(s) \sim& \log(1/(s-1)) \sim \sum_{\mathfrak{p}} N_{\mathfrak{p}}^{-s}\\ \sim&\sum_{\mathfrak{p}}\sum_{f(\mathfrak{p}/p)=1=e(\mathfrak{p}/p)} p^{-s} + \sum_{\mathfrak{p}}\sum_{f(\mathfrak{p}/p)>1} p^{-f(\mathfrak{p}/p)s} + \sum_{\mathfrak{p}}\sum_{f(\mathfrak{p}/p)=1,e(\mathfrak{p}/p)>1} p^{-s}.\end{aligned}$$

The third series is bounded as the number of ramified primes is finite, now the second one is also bounded since:

$$\sum_{\mathfrak{p}}\sum_{f(\mathfrak{p}/p)>1} p^{-f(\mathfrak{p}/p)s} \leq \sum_{\mathfrak{p}}\sum_{f(\mathfrak{p}/p)>1} p^{-2s} \leq [K:\mathbb{Q}]\sum_{p\in\mathcal{S}_K} p^{-2s}.$$

The last inequality comes from the fact that since the extension is Galois, and we are looking at unramified primes, for such a prime ideal, $\mathfrak{p}$, we have $g(\mathfrak{p}/p) =$

$\frac{1}{f(\mathfrak{p}/p)}[K:\mathbb{Q}]$. Thus since $f(\mathfrak{p}/p) > 1$ we get the inequality. So we are left only with the first series

$$\begin{aligned}\log \zeta_K(s) \sim & \log(1/(s-1)) \sim \sum_{\mathfrak{p}} N_{\mathfrak{p}}^{-s} \\ & \sim \sum_{\mathfrak{p}} \sum_{f(\mathfrak{p}/p)=1=e(\mathfrak{p}/p)} p^{-s} \underbrace{=}_{g(\mathfrak{p}/p)=[K:\mathbb{Q}]} [K:\mathbb{Q}] \sum_{p\in\mathcal{S}_K} p^{-s}\end{aligned}$$

Hence

$$\log\left(\frac{1}{s-1}\right) = \sum_{p\in\mathcal{S}_K} [K:\mathbb{Q}]p^{-s} + \underbrace{b(s)}_{\text{bounded as } s\to 1^+}.$$

Thus we can compute $\delta(\mathcal{S}_K)$

$$\begin{aligned}\delta(\mathcal{S}_K) = & \lim_{s\to 1^+} \frac{\sum_{p\in\mathcal{S}_K} p^{-s}}{\log\left(\frac{1}{s-1}\right)} \\ = & \left(\frac{\sum_{p\in\mathcal{S}_K}[K:\mathbb{Q}]p^{-s} + b(s)}{\sum_{p\in\mathcal{S}_K} p^{-s}}\right)^{-1} \\ = & [K:\mathbb{Q}]^{-1}.\end{aligned}$$

□

Remark 1.7 (Notations)**.** Let $\mathcal{S}, \mathcal{T}$ be sets of primes in $\mathcal{O}_K$, where K is a number field. We define the following notations:

- Write $\mathcal{S} \prec \mathcal{T}$ if and only if $\delta(\mathcal{S} - \mathcal{T}) = 0$.
- Write $\mathcal{S} \approx \mathcal{T}$ if and only if $\mathcal{S} \prec \mathcal{T} \prec \mathcal{S}$.

Theorem 1.8. *Let E and K be number fields, both Galois over $\mathbb{Q}$, then*

$$\mathcal{S}_K \prec \mathcal{S}_E \iff E \subseteq K.$$

Proof. The part "$\Longleftarrow$" is clear since if $E \subseteq K$ then $\mathcal{S}_K \subseteq \mathcal{S}_E$.
For "$\Longrightarrow$"suppose that $\mathcal{S}_K \prec \mathcal{S}_E$. We know from exercise 3 sheet 3 that $\mathcal{S}_{KE} = \mathcal{S}_E \cap \mathcal{S}_K$, and since $\delta(\mathcal{S}_K - \mathcal{S}_E) = 0$, using lemma 1.5, we get

$$\delta(\mathcal{S}_{EK}) = \delta(\mathcal{S}_K \cap \mathcal{S}_E) = \delta(\mathcal{S}_K - \mathcal{S}_E) + \delta(\mathcal{S}_E \cap \mathcal{S}_K) = \delta(\mathcal{S}_K).$$

Thus Theorem 1.6 gives us that $[KE:\mathbb{Q}] = [K:\mathbb{Q}]$ hence $KE = K$ and $E \subseteq K$. □

2 Chapter 3 : Ray class group

Our goal in this section is to generalize the Dirichlet argument to a prime ideal in the ring of integers of a number field F. The question we will try to answer

is "Are there infinitely many primes $\mathfrak{p}$ of $\mathcal{O}_F$ in an arithmetic progression ? " But for that, we need to define what we mean by arithmetic progression in this context.

- We will replace "mod m" for $m \in \mathbb{Z}$ with "mod $\mathfrak{m}$" with $\mathfrak{m}$ an ideal of $\mathcal{O}_F$.
- We will define the ray class group analogously to the ideal class group.
- We will also expand the notion of Dirichlet characters and $\mathcal{L}$-functions.

Theorem 2.1 (Approximation Theorem)**.** *Let $|.|_1, ..., |.|_n$ be non-trivial pairwise inequivalent absolute values on F and let $\beta_1, ..., \beta_n$ be non-zero elements of F . For any $\epsilon > 0$, there is an element $\alpha \in F$ such that*

$$|\alpha - \beta_j|_j < \epsilon$$

for each $j = 1, ..., n$.

Proof. We will first show that $\exists x_1, ..., x_n \in F$ so that $\forall j$ we have $|x_j|_j > 1$ and $|x_j|_i < 1$ for all $i \neq j$. We proceed by induction on n.

- For $n = 2$: We take $j = 1$ And since $|.|_1, |.|_2$ are inequivalent, we can find $y \neq z \in F - \{0\}$ such that $|y|_1 > 1 \geq |z|_1$ and $|y|_2 \leq 1 < |z|_2$. Indeed, consider
$$\sup_{z \in F, |z|_1 \leq 1} \{|z|_2|\}$$
then this supremum can't be finite, else if $\exists M$ such that $\forall z \in F$ with$|z|_1 \leq 1$, $|z|_2 \leq M$ we would have, that for all $z \in F$, take $z' = \frac{z}{|z|_1}$ then, $|z'|_1 = 1$ thus $|z'|_2 = \frac{|z|_2}{|z|_1} \leq M$ by homogeneity, which is a contradiction since the two norms are inequivalent. This means that we can find a z as we wanted. For y we simply inverse the two norms and get the same result. Now take $x_1 = \frac{y}{z}$.
- For $n > 1$: Suppose that $\exists x \in F$ such that $|x|_1 > 1$ and $|x|_i < 1$ for all $i = 1, ..., n-1$. by the above, we know that there is a $v \in F$ such that $|v|_1 > 1$ and $|v|_n < 1$. We take x_1 to be :
$$x_1 = \begin{cases} x & \text{if } |x|_n < 1 \\ x^r v & \text{if } |x|_n = 1 \\ \frac{x^r v}{1+x^r} & \text{if } |x|_n > 1. \end{cases}$$
For $r \in \mathbb{Z}$ determined as follows:
  - For $|x|_n = 1$ then it suffices to take a sufficiently large r as $|x_1|_i = |x|_i^r |v|_i \xrightarrow{r \to \infty} 0$.

– For $|x|_n > 1$, we have

$$|x_1|_i = \frac{|x|_i^r |v|_i}{|1+x^r|_i} = \frac{|v|_i}{|x^{-r}+1|_i}.$$

When $2 \leq i \leq n-1$, since $|x|_i < 1$ we have

$$\frac{|v|_i}{|x^{-r}+1|_i} \xrightarrow{r\to\infty} 0.$$

When $i = 1$, since $|x|_1 > 1$ we have:

$$\frac{|v|_1}{|x^{-r}+1|_1} \xrightarrow{r\to\infty} |v|_1 > 1.$$

When $i = n$, since $|x|_n < 1$ we have:

$$\frac{|v|_n}{|x^{-r}+1|_n} \xrightarrow{r\to\infty} |v|_n < 1.$$

Similarly we can find $x_2, ..., x_n$ such that for all j $|x_j|_j > 1$ and $|x_j|_i < 1$ for all $i \neq j$.

Now we set $\alpha = \sum_{j=1}^n \frac{x_j^l \beta_j}{1+x_j^l}$ where $l \in \mathbb{Z}$ is determined as follows:

$$|\alpha\beta_j|_j \leq \underbrace{\left|\frac{\beta_j}{1+x_j^l}\right|_j}_{\approx \frac{1}{|x_j|_j^l} \xrightarrow{l\to\infty} 0} + \sum_{i\neq j} \underbrace{\left|\frac{x_i^l \beta_i}{1+x_i^l}\right|_j}_{\approx |x_i|_j^l \xrightarrow{l\to\infty} 0}.$$

Thus it suffices to choose l large enough. □

Remark 2.2. If we apply the Approximation Theorem 2.1 in the case where the absolute values are the $\mathfrak{p}$-adic norm $|.|_{\mathfrak{p}_1}, ..., |.|_{\mathfrak{p}_n}$, all pairwise inequivalent, and take $\beta_1, ..., \beta_n \in F^\times$ such that $\forall j = 1, ..., n$, $\beta_j \in \mathcal{O}_{\mathfrak{p}_j}^\times$, with $\mathcal{O}_{\mathfrak{p}_j}^\times$ the units of the $\mathfrak{p}$-adic integer, then by the Approximation Theorem, $\forall \epsilon > 0, \exists \alpha \in F$ such that $\forall j = 1, ..., n$

$$|\alpha - \beta_j|_{\mathfrak{p}_j} < \epsilon.$$

Now if we take $\epsilon = c^m$ with $c \in (0,1)$ as in definition of the $\mathfrak{p}_j$-adic norms $|.|_{\mathfrak{p}_j}$ and $m \in \mathbb{Z}$, we have

$$\left|\frac{\alpha}{\beta_j} - 1\right|_{\mathfrak{p}_j} \underbrace{|\beta_j|_{\mathfrak{p}_j}}_{=1} < \epsilon = c^m$$

$$\implies \mathrm{ord}_{\mathfrak{p}_j}\left(\frac{\alpha}{\beta_j} - 1\right) > m$$

$$\implies \frac{\alpha}{\beta_j} - 1 \in \mathfrak{p}_j^m$$

$$\implies \alpha - \beta_j \in \mathfrak{p}_j^m$$

$$\implies \alpha \equiv \beta_j \bmod \mathfrak{p}_j^m.$$

Thus if $F = \mathbb{Q}$ and $\mathfrak{p}_j^m = (p_j)$, $p_j \in \mathbb{Z}$ prime we get the Chinese remainder Theorem.

Definition 2.3. Recall that the ideal class group of a number field F is

$$\mathcal{C}_F = \mathcal{I}_F / \mathcal{P}_F$$

Where $\mathcal{I}_F = \{\text{fractional ideals of } F\}$ and $\mathcal{P}_F = \{\text{fractional principal ideals of } F\}$.

Definition 2.4. Let $\alpha \in F$ be such that $\sigma(\alpha) > 0$, for all σ real embeddings of F. Then we say that α is totally positive and we denote it by $\alpha >> 0$.

Definition 2.5. Let $\mathfrak{m} \subset \mathcal{O}_F$ be a non-zero integral prime ideal, we define

$$\mathcal{P}_{F,\mathfrak{m}}^+ = \text{subgroup of } \mathcal{P}_F \text{ generated by } \{< \alpha >, \alpha \in \mathcal{O}_F, \alpha \equiv 1 \bmod \mathfrak{m}\}.$$

We introduce the following notation for $\alpha \in \mathcal{O}_F$ such that $\alpha \equiv 1 \bmod \mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(\mathfrak{m})}$ for all $\mathfrak{p}|\mathfrak{m}$ in $F_\mathfrak{p}$ then we write $\alpha \overset{\times}{\equiv} 1 \bmod \mathfrak{m}$.

Lemma 2.6. *With this notation, we have that*

$$\begin{aligned}\mathcal{P}_{F,\mathfrak{m}}^+ =& \{< \frac{\alpha}{\beta} > | \alpha, \beta \in \mathcal{O}_F \textit{ prime to } \mathfrak{m}, \frac{\alpha}{\beta} >> 0, \alpha \equiv \beta \bmod \mathfrak{m}\} \\ =& \{< \alpha > | \alpha \in F, \alpha >> 0, \alpha \overset{\times}{\equiv} 1 \bmod \mathfrak{m}\}.\end{aligned}$$

Proof. Exercise 4 sheet 6. □

Definition 2.7. Let $\mathcal{I}_{F,\mathfrak{m}} = \{\mathfrak{a} \in \mathcal{I}_F, \mathrm{ord}_\mathfrak{p}(\mathfrak{a}) = 0, \forall \mathfrak{p}|\mathfrak{m}\}$, then we define the strict ray class group of f for $\mathfrak{m} \subset \mathcal{O}_F$ a non-zero integral prime ideal as :

$$\mathcal{R}_{F,\mathfrak{m}}^+ = \mathcal{I}_{F,\mathfrak{m}} / \mathcal{P}_{F,\mathfrak{m}}^+.$$

Example 2.8. Take $F = \mathbb{Q}, \mathfrak{m} = m\mathbb{Z}, m \geq 1$. If $< r > \in \mathcal{I}_{\mathbb{Q},m}$, then $r = \frac{a}{b} > 0$ such that $(a, m) = (b, m) = 1$. Then we define

$$\begin{aligned}\Phi : \mathcal{I}_{\mathbb{Q},m} &\to \left(\mathbb{Z}/m\mathbb{Z}\right)^\times \\ < r > &\mapsto ab^{-1}.\end{aligned}$$

One can show that this map is surjective and well-defined, with kernel

$$\begin{aligned}\ker \Phi =& \{< r > \in \mathcal{I}_{\mathbb{Q},m} | ab^{-1} \equiv 1 \bmod m\} \\ \underbrace{=}_{\text{Lemma 2.6}}& \mathcal{P}_{\mathbb{Q},m}^+ \\ \implies \mathcal{R}_{\mathbb{Q},m}^+ &= \mathcal{I}_{\mathbb{Q},m} / \mathcal{P}_{\mathbb{Q},m^+} \cong \left(\mathbb{Z}/m\mathbb{Z}\right)^\times.\end{aligned}$$