Reading group term 1 26/27 notes

Simon Shackleton

November 2026

1 Recap

We recall necessary/useful definitions and facts.

1.1 p-adics and places.

Let p be a prime. Consider a sequence of integers $x = (x_1, x_2, ...)$. We say that x is coherent if $x_{n+1} \equiv x_n \mod p^n$. Two such sequences are equivalent if $x_n \equiv y_n \mod p^n$. The p-adic integers are the set of equivalence classes of such sequences. We denote $\mathbb{Z}_p$ the commutative ring of these p-adic integers. We note that $\mathbb{Z}$ is a subring of $\mathbb{Z}_p$ under the embedding $x \mapsto (x, x, ...)$.

If $x, y \in \mathbb{Z}_p$ we say that $y|x$ if there exists $z \in \mathbb{Z}_p$ such that $yz = x$.

Lemma 1.1. *x a p-adic integer. $p^k|x$ iff $p^k|x_k$.*

This follows from using the definition of x being coherent.

We define the p-adic order of a p-adic integer x to be $v_p(x) = \sup\{k : p^k|x\}$. We define its absolute value to be $|x|_p = p^{-v_p(x)}$.

One may check that the p-adic integers form a integral domain. We define $\mathbb{Q}_p$ to be the field of fractions of the piadic integers. We call elements of $\mathbb{Q}_p$ the p-adic numbers. We define the p-adic order of a p-adic number $x = a/b$ where $b \neq 0$ to be $v_p(x) = v_p(a) - v_p(b)$. We define its absolute value to be $|x|_p = |a|_p/|b|_p$. When simply working in $\mathbb{Q}$ we inherit this absolute value where $|a/b| = p^{-ord_p(x)}$ where $ord_p(x)$ is the unique number such that $x = p^{ord_p(x)}a/b$ with a and b both coprime to p.

Lemma 1.2. *x a p-adic integer is a unit iff $p \nmid x$.*

It follows from this that every p-adic number may be written as $p^m u$ where m is an integer and u a unit in the p-adic integers.

An absolute value $|.|$ on a field K is a non-negative function satisfying: $|x| = 0$ iff $x = 0$, $|x \cdot y| = |x||y|$ and $|x + y| \leq |x| + |y|$. Any field has the trivial absolute value $|x| = 1$ $(x \neq 0)$. We say that the absolute value is *non-archimedian* if it satisfies the untra metric inequality i.e for all $x, y \in K$ $|x + y| \leq \max\{|x|, |y|\}$. Otherwise $|\cdot|$ is simply called *archimedian*. The p-adic absolute value is non-archimedian.

A **place** v is an equivalence class of non-trivial absolute values. By $|\cdot|_v$ we mean some absolute value in the equivalence class of v. If the field L is an extension of K and v is a place of K we write $w|v$ for a place w of L iff the restriction to K of any representative of w is a representative of v. i.e w extends v. The completion of K with respect to the place v is an extension field k_v with a place w such that:

- $w|v$.
- The topology of K induced by w is complete.
- K is dense in K_v.

The only complete archimedian fields are $\mathbb{R}$ or $\mathbb{C}$. The field $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to p.

For a generic number field k, M_k consists of all the absolute values of k whose restriction to $\mathbb{Q}$ is one of the standard absolute values on $\mathbb{Q}$ (these being $|\cdot|_\infty$ and the p-adic absolute values $|\cdot|_p$). One writes M_k^∞ the set of archimedian absolute values and M_k^0 the set of non-archimedian absolute values. Note that the absolute values in $\mathbb{Q}$ satisfy $\prod_{v\in M_\mathbb{Q}} |x|_v = 1$ for $x \neq 0$. This follows simply from prime decomposition.

The relative Weil height of an algebraic number β relative to some number field K is

$$H_K(\beta) := \prod_{v\in M_k} \max\{1, |\beta|_v\}^{n_v} \tag{1}$$

where $n_v = [K_v : \mathbb{Q}_w]$ such that $v|w$.

2 Subspace Theorem

2.1 Recap

First we recall Roth's theorem

Theorem 2.1. *Fix $\epsilon > 0$. Let K be a number field and $S \subset M_K$ a finite set of places. For each $v \in S$ let $\alpha_v \in K_v$ be K algebraic. Then there are only finitely many $\beta \in K$ such that*

$$\prod_{v\in S} \min\{1, |\alpha - \beta|_v\} \leq H(\beta)^{-2-\epsilon} \tag{2}$$

Remark. *In particular we can take $K = \mathbb{Q}$ and $S = \{\infty\}$ to get an improved Louiville.*

Remark. *We have discussed that Roth's is ineffective in the sense that it does not provide and upper bound on the height of β but is effective in the number of solutions. We will see that the 'same' thing holds for the subspace theorem.*

Now some notation.

For a place v we denote by$|\cdot|_v$ the normalized absolute value $|x|_v := |N_{K_v/\mathbb{Q}_p}(x)|_p^{1/[K:\mathbb{Q}]}$ for $x \in K$ and $v|p$. We similarly denote $|.|_v$ its extension to the completion K_v. K a number field, then M_K satisfies the product formula .i.e if $\prod_{v\in M_K} |x|_v = 1$ for any $x \in K \setminus \{0\}$.

The multiplicative height of an algebraic number α is $H(\alpha) = \prod_{v\in M_v} \max\{1, |\alpha|_v\}^{n_v}$ with $n_v = [K_v : \mathbb{Q}_w]$ and $v|w$.

The multiplicative height of on algebraic points of $\mathbb{P}^n_{\overline{\mathbb{Q}}}$ P $H(\underline{x}) = \prod_{v\in M_v} \max_j |x_j|_v$ where P where P is represented by a homogeneous non-zero vector $\underline{x}$ with coordinates in some number field K. For $\underline{x} \in K^{n+1}$ we take $|\underline{x}|_v$ to be $\max_j |x_j|_v$.

2.2 Statement

Theorem 2.2 (Subspace Theorem)**.** *K a number field and $S \subset M_K$ a finite set of places, $n \in \mathbb{N}$ and $\epsilon > 0$. For each $v \in S$ we take $L_{0v}, ..., L_{nv}$ to be a linearly independent set of linear forms in the variables $X_0, ..., X_n$ with K-algebraic coefficients in K_v. Then there are finitely many hyperplanes $T_1, ..., T_h$ of $\mathbb{P}^n_K$ such that the set of solutions $\mathbb{P}^n_K(K)$ (these are the K- rational points of that space) of*

$$\prod_{v \in S} \prod_{i=0}^{n} \frac{|L_{iv}(\underline{x})|_v}{|\underline{x}|_v} < H(\underline{x})^{-n-1-\epsilon} \tag{3}$$

are contained in $T_1 \cup ... \cup T_h$.

Remark. *No bound may be placed a priori on the height of the infinitely many subspaces but we have an effective bound for the number of subspaces containing solutions.*

We give an equivalent formulation for affine space.

Theorem 2.3. *K, S and each L_{iv} as before with S containing each of the archimedian places. Let $\epsilon > 0$. Then there are finitely many hyperplanes $T_1, ..., T_h$ of K^{n+1} such that the set of S-integral solutions $\underline{x} \in \mathcal{O}^{n+1}_{S,K}/\{0\}$ equation*

$$\prod_{v \in S} \prod_{i=0}^{n} |L_{iv}(\underline{x})|_v < H(\underline{x})^{-\epsilon} \tag{4}$$

are contained in $T_1 \cup ... \cup T_h$.

2.3 Example

Example 1. We now show that the case $n = 1$ yields Roth's theorem, hence justifying why we call this a generalisation.

By splitting the solutions to the inequality in Roth's theorem into a finite set of places S^* according to the v such that $|\alpha_v - \beta|_v < 1$ for $v \in S^*$, We can clearly see that Roth's theorem may equivalently be formulated as the number of solutions to

$$\prod_{v \in S^*} |\alpha_v - \beta|_v < H(\beta)^{-2-\epsilon} \tag{5}$$

form a finite set. where $S^* \subset S$ chosen such that $|\alpha_v - \beta|_v < 1$ for $v \in S^*$.

We choose $L_{0v} = X_0$ and $L_{1v} = X_1 - \alpha_v X_0$. Choosing $\underline{x} = (1 : \beta) \in \mathbb{P}^1(K)$ we see that

$$\frac{|L_{0v}(\underline{x})|_v}{|\underline{x}|_v} \frac{|L_{1v}(\underline{x})|_v}{|\underline{x}|_v} = |\beta - \alpha_v| \max\{1, |\beta|_v\}^{-2} \tag{6}$$

from definition of norm in K^2. Now we note that if $|\beta - \alpha_v|_v < 1$ then by the reverse triangle inequality $|\beta| < 1 + |\alpha_v|_v$ and so $\max\{1, |\beta|_v\}^{-2}$ may be bounded independently of β. i.e $\max\{1, |\beta|_v\}^{-2} \geq C$ for some absolute constant C. So to yield Roth's we need only show that

$$\prod_{v \in S^*} \frac{|L_{0v}(\underline{x})|_v}{|\underline{x}|_v} \frac{|L_{1v}(\underline{x})|_v}{|\underline{x}|_v} < CH(\underline{x})^{-2-\epsilon} \tag{7}$$

To show this we may appeal to Northcott's theorem. This states that There are only finitely many algebraic numbers of bounded degree and bounded height. As each β lies in K we therefore have that $C < H(\underline{x})^{\epsilon/2} = H(\beta)^{\epsilon/2}$for all but finitely many $\beta \in K$. Thus we may apply the subspace theorem with $n = 1$ and $\epsilon/2$ in place of ϵ and conclude that the solutions β form a finite set. Roth's theorem follows.

2.4 application to S-units

Theorem 2.4. *Let K be a number field and let S be a finite set of places of K containing all archimedean places, with group of S -units $U_{S,K}$. Let χ be the set of solutions of*

$$x_1 + ... + x_n = 1 \tag{8}$$

such that $(x_1, ..., x_n) \in (U_{S,K})^n$ and no proper subsum of $x_1 + ... + x_n$ vanishes. Then χ is finite.

Proof. Quickly recall that $U_{S,K} = \mathcal{O}_{k,s}^*$ where $\mathcal{O}_{k,s} := \{x \in k : |x|_v \leq 1 \text{ for all } v \in M_K^0 \setminus S\}$. We proceed by induction. Clearly if $n = 1$ then then the only solution is $x_1 = 1$ and the result is obvious.

We say that a solution $x \in X$ of the S-unit equation $x_1 + ... + x_n = 1$ is nondegenerate if no proper subsum of $x_1 + ... + x_n$ vanishes. We partition X into finitely many subsets according to the set of indices $j_v (v \in S)$ such that

$$j_v := \min\{j : |x_j|_v = \max_i |x_i|_v\} \tag{9}$$

and then it suffices to prove the result for each subset.

We fix one of these subsets, say $\chi^{'}$ and we deine linear forms $L_j v = X_j$ for $j \neq j_v$ and $L_{j_v v} = X_1 + ... + X_n$. As $L_{j_v v}(\underline{x}) = x_1 + ... + x_n = 1$ and $|x_{j_v}|_v = |\underline{x}|_v$ we have that

$$\prod_{j=1}^{n} L_{jv}(\underline{x}) = \prod_{j \neq j_v} |x_j|_v = |\underline{x}|_v^{-1} \prod_j |x_j|_v \tag{10}$$

note also that for every j

$$\prod_{v \in S} |x_j| = 1 \tag{11}$$

where we have used that $x_j \in U_{S,K}$ so $|x|_v = 1$ for v not in S and the product rule. So we have

$$\prod_{v \in S} \prod_{j=1}^{n} L_{jv}(\underline{x}) = \prod_{v \in S} |\underline{x}|_v^{-1} \tag{12}$$

Moreover, we have

$$H(\underline{x}) = \prod_{v \in M_K} |\underline{x}|_v = \prod_{v \in S} |\underline{x}|_v \tag{13}$$

so we have

$$\prod_{v \in S} \prod_{j=1}^{n} L_{jv}(\underline{x}) = H(\underline{x})^{-1} \tag{14}$$

and now applying the subspace theorem (affine version) with $\epsilon = 1$ we see that the solutions $\underline{x} \in \chi^{'}$ to the above equation lie in a finite union of proper linear subspaces in K^n . Now we partition $\chi^{'}$ into finitely many subsets, such that in a typical subset $\chi^{''}$ we have a relation $\sum a_i x_i = 0$. Here we are just using what it means for our solutions to live in a hyperplane. We may assume after a permuation of coordinates that $a_n \neq 0$. We may then, using that $x_1 + ...x_n = 1$, eliminate x_n, to arrive at the relation

$$b_1 x_1 + ... + b_{n-1} x_{n-1} = 1 \tag{15}$$

for $b_i \in K$ not all 0. By removing vanishing subsums from the above relation, we end up with a new relation $\sum_{i \in I} b_i x_i = 1$. Here $I \subset 1, .., n$ of size at most $n - 1$ where no proper subsum vanishes. Thus by partitioning once again $\chi^{''}$ into finitely many subsets, it suffices to deal with one such relation.

We are close to using the induction hypothesis, it would be ideal to make each $b_i x_i$ into an S-unit somehow. We do just this. For any non-zero element of K it is possible to extend S such that the element is a S-unit. So we enlarge S to $S^{'}$ so that each b_i with $i \in I$ is a $S^{'}-$unit. We obtain a non-degenerate solution $\underline{y}$ in $S^{'}$-units, $y_i = b_i x_i$ such that

$$\sum_{i \in I} y_i = 1 \tag{16}$$

Since $|I| \leq n-1$, the induction hypothesis shows that the $b_i x_i$ $(i \in I)$, and hence the coordinates $x_i (i \in I)$ themselves belong to a finite set. Thus we have proved that the inductive hypothesis implies that there is a finite set Φ such that any solution $x \in X$ has at least one coordinate in Φ. Let $x_{i_0} = c, c \in \Phi$, be one of these relations. Then $c \neq 1$ because $\underline{x}$ is a non-degenerate solution. By enlarging S to a new set $S^{''}$ so that $1-c$ becomes an $S^{''}$-unit and setting $z_i = (1-c)^{-1} x_i$, we have that $z_i = (1-c)^{-1} x_i, (i \neq i_0)$ is an $S^{''}$-unit and yields a non-degenerate solution of

$$\sum_{i \neq i_0} z_i = 1. \tag{17}$$

Thus we can apply induction again to conclude that all remaining coordinates x_i also belong to a finite set.

□