Math 129: Algebraic Number Theory
Lecture 18: Independence, Finite Residue Field Case

William Stein

Tuesday, April 13, 2004

6 Independence

The following theorem asserts that inequivalent valuations are in fact almost totally indepedent. For our purposes it will be superseded by the result of Section 15.

Theorem 6.1 (Weak Approximation). *Let $|\cdot|_n$, for $1 \leq n \leq N$, be inequivalent nontrivial valuations of a field K. For each n, let K_n be the topological space consisting of the set of elements of K with the topology induced by $|\cdot|_n$. Let Δ be the image of K in the topological product*

$$A = \prod_{1 \leq n \leq N} K_n$$

equipped with the product topology. Then Δ is dense in A.

The conclusion of the theorem may be expressed in a less topological manner as follows: given any $a_n \in K$, for $1 \leq n \leq N$, and real $\varepsilon > 0$, there is an $b \in K$ such that simultaneously

$$|a_n - b|_n < \varepsilon \qquad (1 \leq n \leq N).$$

If $K = \mathbf{Q}$ and the $|\cdot|$ are p-adic valuations, Theorem 6.1 is related to the Chinese Remainder Theorem, but the strong approximation theorem is the real generalization. This theorem involves adeles, so we cill not state it until later.

Proof. We note first that it will be enough to find, for each n, an element $c_n \in K$ such that

$$|c_n|_n > 1 \quad \text{and} \quad |c_n|_m < 1 \quad \text{for } n \neq m,$$

where $1 \leq n, m \leq N$. For then as $r \to +\infty$, we have

$$\frac{c_n^r}{1+c_n^r} = \frac{1}{1+\left(\frac{1}{c_n}\right)^{-r}} \to \begin{cases} 1 & \text{with respect to } |\cdot|_n \text{ and} \\ 0 & \text{with respect to } |\cdot|_m, \text{ for } m \neq n. \end{cases}$$

It is then enough to take

$$b = \sum_{n=1}^{N} \frac{c_n^r}{1 + c_n^r} \cdot a_n$$

By symmetry it is enough to show the existence of $c = c_1$ with

$$|c|_1 > 1 \qquad \text{and} \qquad |c|_n < 1 \quad \text{for} \quad 2 \le n \le N.$$

We will do this by induction on N.

First suppose $N = 2$. Since $|\cdot|_1$ and $|\cdot|_2$ are inequivalent (and all absolute values are assumed nontrivial) there is an $a \in K$ such that

$$|a|_1 < 1 \qquad \text{and} \qquad |a|_2 \ge 1$$

and similarly a b such that

$$|b|_1 \ge 1 \qquad \text{and} \qquad |b|_2 < 1.$$

Then $c = \dfrac{b}{a}$ will do.

Next suppose $N \ge 3$. By the case $N - 1$, there is an $a \in K$ such that

$$|a|_1 > 1 \qquad \text{and} \qquad |a|_n < 1 \quad \text{for} \quad 2 \le n \le N - 1.$$

By the case for $N = 2$ there is a $b \in K$ such that

$$|b|_1 > 1 \qquad \text{and} \qquad |b|_N < 1.$$

Then put

$$c = \begin{cases} a & \text{if } |a|_N < 1 \\ a^r \cdot b & \text{if } |a|_N = 1 \\ \dfrac{a^r}{1 + a^r} \cdot b & \text{if } |a|_N > 1 \end{cases}$$

where $r \in \mathbf{Z}$ is sufficiently large so that $|c|_1 > 1$ and $|c|_n < 1$ for $2 \le n \le N$. □

Example 6.2. Suppose $K = \mathbf{Q}$, let $|\cdot|_1$ be the archimedean absolute value and let $|\cdot|_2$ be the 2-adic absolute value. Let $a_1 = -1$, $a_2 = 8$, and $\varepsilon = 1/10$, as in the remark right after Theorem 6.1. Then the theorem implies that there is an element $b \in \mathbf{Q}$ such that

$$|-1 - b|_1 < \frac{1}{10} \qquad \text{and} \qquad |8 - b|_2 < \frac{1}{10}.$$

As in the proof of the theorem, we can find such a b by finding a $c_1, c_2 \in \mathbf{Q}$ such that $|c_1|_1 > 1$ and $|c_1|_2 < 1$, and a $|c_2|_1 < 1$ and $|c_2|_2 > 1$. For example, $c_1 = 2$ and $c_2 = 1/2$ works, since $|2|_1 = 2$ and $|2|_2 = 1/2$ and $|1/2|_1 = 1/2$ and $|1/2|_2 = 2$. Again following the proof, we see that for sufficiently large r we can take

$$\begin{aligned} b_r &= \frac{c_1^r}{1 + c_1^r} \cdot a_1 + \frac{c_2^r}{1 + c_2^r} \cdot a_2 \\ &= \frac{2^r}{1 + 2^r} \cdot (-1) + \frac{(1/2)^r}{1 + (1/2)^r} \cdot 8. \end{aligned}$$

We have $b_1 = 2$, $b_2 = 4/5$, $b_3 = 0$, $b_4 = -8/17$, $b_5 = -8/11$, $b_6 = -56/55$. None of the b_i work for $i < 6$, but b_6 works.

7 Finite Residue Field Case

Let K be a field with a non-archimedean valuation $v = |\cdot|$. Recall that the set of $a \in K$ with $|a| \leq 1$ forms a ring $\mathcal{O}$, the ring of integers for v. The set of $u \in K$ with $|u| = 1$ are a group U under multiplication, the group of units for v. Finally, the set of $a \in K$ with $|a| < 1$ is a maximal ideal $\mathfrak{p}$, so the quotient ring $\mathcal{O}/\mathfrak{p}$ is a field. In this section we consider the case when $\mathcal{O}/\mathfrak{p}$ is a finite field of order a prime power q. For example, K could be $\mathbf{Q}$ and $|\cdot|$ could be a p-adic valuation, or K could be a number field and $|\cdot|$ could be the valuation corresponding to a maximal ideal of the ring of integers. Among other things, we will discuss in more depth the topological and measure-theoretic nature of the completion of K at v.

Suppose further for the rest of this section that $|\cdot|$ is discrete. Then (as we proved before), the ideal $\mathfrak{p}$ is a principal ideal (π), say, and every $a \in K$ is of the form $a = \pi^n \varepsilon$, where $n \in \mathbf{Z}$ and $\varepsilon \in U$ is a unit. We call

$$n = \mathrm{ord}(a) = \mathrm{ord}_\pi(a) = \mathrm{ord}_\mathfrak{p}(a) = \mathrm{ord}_v(a)$$

the ord of a at v. (Some authors, including me (!) also call this integer the *valuation* of a with respect to v.) If $\mathfrak{p} = (\pi')$, then π/π' is a unit, and conversely, so $\mathrm{ord}(a)$ is independent of the choice of π.

Let $\mathcal{O}_v$ and $\mathfrak{p}_v$ be defined with respect to the completion K_v of K at v.

Lemma 7.1. *There is a natural isomorphism*

$$\varphi : \mathcal{O}_v/\mathfrak{p}_v \to \mathcal{O}/\mathfrak{p},$$

and $\mathfrak{p}_v = (\pi)$ as an $\mathcal{O}_v$-ideal.

Proof. We may view $\mathcal{O}_v$ as the set of equivalence classes of Cauchy sequences (a_n) in K such that $a_n \in \mathcal{O}$ for n sufficiently large. For any ε, given such a sequence (a_n), there is N such that for $n, m \geq N$, we have $|a_n - a_m| < \varepsilon$. In particular, we can choose N such that $n, m \geq N$ implies that $a_n \equiv a_m \pmod{\mathfrak{p}}$. Let $\varphi((a_n)) = a_N \pmod{\mathfrak{p}}$, which is well-defined. The map φ is surjective because the constant sequences are in $\mathcal{O}_v$. Its kernel is the set of Cauchy sequences whose elements are eventually all in $\mathfrak{p}$, which is exactly $\mathfrak{p}_v$. This proves the first part of the lemma. The second part is true because any element of $\mathfrak{p}_v$ is a sequence all of whose terms are eventually in $\mathfrak{p}$, hence all a multiple of π (we can set to 0 a finite number of terms of the sequence without changing the equivalence class of the sequence). □

Assume for the rest of this section that K is complete with respect to $|\cdot|$.

Lemma 7.2. *Then ring $\mathcal{O}$ is precisely the set of infinite sums*

$$a = \sum_{j=0}^{\infty} a_j \cdot \pi^j \tag{7.1}$$

where the a_j run independently through some set $\mathcal{R}$ of representatives of $\mathcal{O}$ in $\mathcal{O}/\mathfrak{p}$.

By (7.1) is meant the limit of the Cauchy sequence $\sum_{j=0}^{n} a_j \cdot \pi^j$ as $j \to \infty$.

Proof. There is a uniquely defined $a_0 \in \mathcal{R}$ such that $|a - a_0| < 1$. Then $a' = \pi^{-1} \cdot (a - a_0) \in \mathcal{O}$. Now define $a_1 \in \mathcal{R}$ by $|a' - a_1| < 1$. And so on. □

Example 7.3. Suppose $K = \mathbf{Q}$ and $|\cdot| = |\cdot|_p$ is the p-adic valuation, for some prime p. We can take $\mathcal{R} = \{0, 1, \ldots, p-1\}$. The lemma asserts that

$$\mathcal{O} = \mathbf{Z}_p = \left\{ \sum_{j=0}^{\infty} a_n p^n : 0 \le a_n \le p-1 \right\}.$$

Notice that $\mathcal{O}$ is uncountable since there are p choices for each p-adic "digit". We can do arithmetic with elements of $\mathbf{Z}_p$, which can be thought of "backwards" as numbers in base p. For example, with $p = 3$ we have

$$\begin{aligned}
&(1 + 2 \cdot 3 + 3^2 + \cdots) + (2 + 2 \cdot 3 + 3^2 + \cdots) \\
&= 3 + 4 \cdot 3 + 2 \cdot 3^2 + \cdots \qquad \text{not in canonical form} \\
&= 0 + 2 \cdot 3 + 3 \cdot 3 + 2 \cdot 3^2 + \cdots \qquad \text{still not canonical} \\
&= 0 + 2 \cdot 3 + 0 \cdot 3^2 + \cdots
\end{aligned}$$

Basic arithmetic with the p-adics in MAGMA is really weird (even weirder than it was a year ago... There are presumably efficiency advantages to using the MAGMA formalization, and it's supposed to be better for working with extension fields. But I can't get it to do even the calculation below in a way that is clear.) In PARI (gp) the p-adics work as expected:

```
? a = 1 + 2*3 + 3^2 + O(3^3);
? b = 2 + 2*3 + 3^2 + O(3^3);
? a+b
%3 = 2*3 + O(3^3)
? sqrt(1+2*3+O(3^20))
%5 = 1 + 3 + 3^2 + 2*3^4 + 2*3^7 + 3^8 + 3^9 + 2*3^10 + 2*3^12
       + 2*3^13 + 2*3^14 + 3^15 + 2*3^17 + 3^18 + 2*3^19 + O(3^20)
? 1/sqrt(1+2*3+O(3^20))
%6 = 1 + 2*3 + 2*3^2 + 2*3^7 + 2*3^10 + 2*3^11 + 2*3^12 + 2*3^13
       + 2*3^14 + 3^15 + 2*3^16 + 2*3^17 + 3^18 + 3^19 + O(3^20)
```

Theorem 7.4. *Under the conditions of the preceding lemma, $\mathcal{O}$ is compact with respect to the $|\cdot|$-topology.*

Proof. Let V_λ, for λ running through some index set Λ, be some family of open sets that cover $\mathcal{O}$. We must show that there is a finite subcover. We suppose not.

Let $\mathcal{R}$ be a set of representatives for $\mathcal{O}/\mathfrak{p}$. Then $\mathcal{O}$ is the union of the finite number of cosets $a + \pi\mathcal{O}$, for $a \in \mathcal{R}$. Hence for at lest one $a_0 \in \mathcal{R}$ the set $a_0 + \pi\mathcal{O}$ is not covered by finitely many of the V_λ. Then similarly there is an $a_1 \in \mathcal{R}$ such that $a_0 + a_1\pi + \pi^2\mathcal{O}$ is not finitely covered. And so on. Let

$$a = a_0 + a_1\pi + a_2\pi^2 + \cdots \in \mathcal{O}.$$

Then $a \in V_{\lambda_0}$ for some $\lambda_0 \in \Lambda$. Since V_{λ_0} is an open set, $a + \pi^J \cdot \mathcal{O} \subset V_{\lambda_0}$ for some J (since those are exactly the open balls that form a basis for the topology). This is a contradiction because we constructed a so that none of the sets $a + \pi^n \cdot \mathcal{O}$, for each n, are not covered by any finite subset of the V_λ. □

Definition 7.5 (Locally compact). A topological space X is *locally compact* at a point x if there is some compact subset C of X that contains a neighborhood of x. The space X is locally compact if it is locally compact at each point in X.

Corollary 7.6. *The complete local field K is locally compact.*

Proof. If $x \in K$, then $x \in C = x + \mathcal{O}$, and C is a compact subset of K by Theorem 7.4. Also C contains the neighborhood $x + \pi\mathcal{O} = B(x, 1)$ of x. Thus K is locally compact at x. □

Remark 7.7. The converse is also true. If K is locally compact with respect to a non-archimedean valuation $|\cdot|$, then

1. K is complete,
2. the residue field is finite, and
3. the valuation is discrete.

For there is a compact neighbourhood C of 0. Then $\pi^n \cdot \mathcal{O} \subset C$ for sufficiently large n, so $\pi^n \cdot \mathcal{O}$ is compact, being closed. Hence $\mathcal{O}$ is compact. Since $|\cdot|$ is a metric, $\mathcal{O}$ is sequentially compact, i.e., every fundamental sequence in $\mathcal{O}$ has a limit, which implies (1). Let a_λ (for $\lambda \in \Lambda$) be a set of representatives in $\mathcal{O}$ of $\mathcal{O}/\mathfrak{p}$. Then $\mathcal{O}_\lambda = \{z : |z - a_\lambda| < 1\}$ is an open covering of $\mathcal{O}$. Thus (2) holds since $\mathcal{O}$ is compact. Finally, $\mathfrak{p}$ is compact, being a closed subset of $\mathcal{O}$. Let S_n be the set of $a \in K$ with $|a| < 1 - 1/n$. Then S_n (for $1 \leq n < \infty$) is an open covering of $\mathfrak{p}$, so $\mathfrak{p} = S_n$ for some n, i.e., (3) is true.

If we allow $|\cdot|$ to be archimedean the only further possibilities are $k = \mathbf{R}$ and $k = \mathbf{C}$ with $|\cdot|$ equivalent to the usual absolute value.

We denote by K^+ the commutative topological group whose points are the elements of K, whose group law is addition and whose topology is that induced by $|\cdot|$. General theory tells us that there is an invariant measure (the Haar measure) defined on K^+ and that this measure is unique up to a multiplicative constant. We now deduce what any such measure μ must be.

First, since μ is invariant,

$$\mu_n = \mu(a + \pi^n\mathcal{O})$$

is independent of a. Further,

$$a + \pi^n \mathcal{O} = \bigcup_{1 \le j \le q} a + \pi^n a_j + \pi^{n+1} \mathcal{O}, \qquad \text{(disjoint union)}$$

where a_j (for $1 \le j \le q$) is a set of representatives of $\mathcal{O}/\mathfrak{p}$. Hence

$$\mu_n = q \cdot \mu_{n+1}.$$

If we normalize μ by putting

$$\mu(\mathcal{O}) = 1$$

we have $\mu_0 = 1$, hence $\mu_1 = q$, and in general

$$\mu_n = q^{-n}.$$

Conversely, without the theory of Haar measure, we could *define* μ to be the necessarily unique measure on K^+ such that $\mu(\mathcal{O}) = 1$ that is translation invariant. This would have to be the μ we just found above.

Everything so far in this section has depended not on the valuation $|\cdot|$ but only on its equivalence class. The above considerations now single out one valuation in the equivalence class as particularly important.

Definition 7.8 (Normalized valuation). Let K be a field equipped with a discrete valuation $|\cdot|$ and residue class field with $q < \infty$ elements. We say that $|\cdot|$ is normalized if

$$|\pi| = \frac{1}{q},$$

where $\mathfrak{p} = (\pi)$ is the maximal ideal of $\mathcal{O}$.

Example 7.9. The normalized valuation on the p-adic numbers $\mathbf{Q}_p$ is $|u \cdot p^n| = p^{-n}$, where u is a rational number whose numerator and denominator are coprime to p.

Next suppose $K = \mathbf{Q}_p(\sqrt{p})$. Then the p-adic valuation on $\mathbf{Q}_p$ extends uniquely to one on K such that $\left|\sqrt{p}\right|^2 = |p| = 1/p$. Since $\pi = \sqrt{p}$ for K, this valuation is not normalized. (Note that the ord of $\pi = \sqrt{p}$ is $1/2$.) The normalized valuation is $v = |\cdot|' = |\cdot|^2$. Note that $|\cdot|' p = 1/p^2$, or $\mathrm{ord}_v(p) = 2$ instead of 1.

Finally suppose that $K = \mathbf{Q}_p(\sqrt{q})$ where $x^2 - q$ has not root mod p. Then the residue class field degree is 2, and the normalized valuation must satisfy $\left|\sqrt{q}\right| = 1/p^2$.

The following proposition makes clear why this is the best choice of normalization.

Theorem 7.10. *Suppose further that K is complete with respect to the normalized valuation $|\cdot|$. Then*

$$\mu(a + b\mathcal{O}) = |b|,$$

where μ is the Haar measure on K^+ normalized so that $\mu(\mathcal{O}) = 1$.

Proof. Since μ is translation invariant, $\mu(a + b\mathcal{O}) = \mu(b\mathcal{O})$. Write $b = u \cdot \pi^n$, where u is a unit. Then since $u \cdot \mathcal{O} = \mathcal{O}$, we have

$$\mu(b\mathcal{O}) = \mu(u \cdot \pi^n \cdot \mathcal{O}) = \mu(\pi^n \cdot u \cdot \mathcal{O}) = \mu(\pi^n \cdot \mathcal{O}) = q^{-n} = |\pi^n| = |b|\,.$$

Here we have $\mu(\pi^n \cdot \mathcal{O}) = q^{-n}$ by the discussion before Definition 7.8. □

We can express the result of the theorem in a more suggestive way. Let $b \in K$ with $b \neq 0$, and let μ be a Haar measure on K^+ (not necessarily normalized as in the theorem). Then we can define a new Haar measure μ_b on K^+ by putting $\mu_b(E) = \mu(bE)$ for $E \subset K^+$. But Haar measure is unique up to a multiplicative constant and so $\mu_b(E) = \mu(bE) = c \cdot \mu(E)$ for all measurable sets E, where the factor c depends only on b. Putting $E = \mathcal{O}$, shows that the theorem implies that c is just $|b|$, when $|\cdot|$ is the normalized valuation.

Remark 7.11. The theory of locally compact topological groups leads to the consideration of the dual (character) group of K^+. It turns out that it is isomorphic to K^+. We do not need this fact for class field theory, so do not prove it here. For a proof and applications see Tate's thesis or Lang's *Algebraic Numbers*, and for generalizations see Weil's *Adeles and Algebraic Groups* and Godement's Bourbaki seminars 171 and 176. The determination of the character group of K^* is local class field theory.

The set of nonzero elements of K form a group K^* under multiplication. Multiplication and inverses are continuous with respect to the topology induced on K^* as a subset of K, so K^* is a topological group with this topology. We have

$$U_1 \subset U \subset K^*$$

where U is the group of units of $\mathcal{O} \subset K$ and U_1 is the group of 1-units, i.e., those units $\varepsilon \in U$ with $|\varepsilon - 1| < 1$, so

$$U_1 = 1 + \pi\mathcal{O}.$$

The set U is the open ball about 0 of radius 1, so is open, and because the metric is nonarchimedean U is also closed. Likewise, U_1 is both open and closed.

The quotient $K^*/U = \{\pi^n \cdot U : n \in \mathbf{Z}\}$ is isomorphic to the additive group $\mathbf{Z}^+$ of integers with the discrete topology, where the map is

$$\pi^n \cdot U \mapsto n \qquad \text{for } n \in \mathbf{Z}.$$

The quotient U/U_1 is isomorphic to the multiplicative group $\mathbf{F}^*$ of the nonzero elements of the residue class field, where the finite gorup $\mathbf{F}^*$ has the discrete topology. Note that $\mathbf{F}^*$ is cyclic of order $q-1$, and Hensel's lemma implies that K^* contains a primitive $(q-1)$th root of unity ζ. Thus K^* has the following structure:

$$K^* = \{\pi^n \zeta^m \varepsilon : n \in \mathbf{Z}, m \in \mathbf{Z}/(q-1)\mathbf{Z}, \varepsilon \in U_1\} \cong \mathbf{Z} \times \mathbf{Z}/(q-1)\mathbf{Z} \times U_1.$$

(How to apply Hensel's lemma: Let $f(x) = x^{q-1} - 1$ and let $a \in \mathcal{O}$ be such that a mod $\mathfrak{p}$ generates K^*. Then $|f(a)| < 1$ and $|f'(a)| = 1$. By Hensel's lemma there is a $\zeta \in K$ such that $f(\zeta) = 0$ and $\zeta \equiv a \pmod{\mathfrak{p}}$.)

Since U is compact and the cosets of U cover K, we see that K^* is locally compact.

Lemma 7.12. *The additive Haar measure μ on K^+, when restricted to U_1 gives a measure on U_1 that is also invariant under multiplication, so gives a Haar measure on U_1.*

Proof. It suffices to show that

$$\mu(1+\pi^n\mathcal{O}) = \mu(u\cdot(1+\pi^n\mathcal{O})),$$

for any $u \in U_1$ and $n > 0$. Write $u = 1 + a_1\pi + a_2\pi^2 + \cdots$. We have

$$\begin{aligned} u\cdot(1+\pi^n\mathcal{O}) &= (1+a_1\pi+a_2\pi^2+\cdots)\cdot(1+\pi^n\mathcal{O}) \\ &= 1+a_1\pi+a_2\pi^2+\cdots+\pi^n\mathcal{O} \\ &= a_1\pi+a_2\pi^2+\cdots+(1+\pi^n\mathcal{O}), \end{aligned}$$

which is an additive translate of $1+\pi^n\mathcal{O}$, hence has the same measure. □

Thus μ gives a Haar measure on K^* by translating U_1 around to cover K^*.

Lemma 7.13. *The topological spaces K^+ and K^* are totally disconnected (the only connected sets are points).*

Proof. The proof is the same as the proof I mentioned last time. The point is that the non-archimedean triangle inequality forces the complement an open disc to be open, hence any set with at least two distinct elements "falls apart" into a disjoint union of two disjoint open subsets. □

Remark 7.14. Note that K^* and K^+ are locally isomorphic if K has characteristic 0. We have the exponential map

$$a \mapsto \exp(a) = \sum_{n=0}^{\infty} \frac{a^n}{n!}$$

defined for all sufficiently small a with its inverse

$$\log(a) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}(a-1)^n}{n},$$

which is defined for all a sufficiently close to 1.