Math 129: Algebraic Number Theory
Lecture 17: Topology, Completeness

William Stein

Thursday, April 8, 2004

Before starting Section 4, I discuss a question from last time...

Remark 2.1. This definition differs from the one on page 46 of [Cassels-Frohlich, Ch. 2] in two ways. First, we assume that $c > 1$ instead of $c < 1$, since otherwise $|\cdot|_p$ does not satisfy Axiom 3 of a valuation. Here's why: Recall that Axiom 3 for a non-archimedean valuation on K asserts that whenever $a \in K$ and $|a| \leq 1$, then $|a+1| \leq 1$. Set $a = p-1$, where $p = p(t) \in K[t]$ is an irreducible polynomial. Then $|a| = c^0 = 1$, since $\mathrm{ord}_p(p-1) = 0$. However, $|a+1| = |p-1+1| = |p| = c^1 < 1$, since $\mathrm{ord}_p(p) = 1$. If we take $c > 1$ instead of $c < 1$, as I propose, then $|p| = c^1 > 1$, as required.

4 Topology

A valuation $|\cdot|$ on a field K induces a topology in which a basis for the neighborhoods of a are the *open balls*

$$B(a,d) = \{x \in K : |x-a| < d\}$$

for $d > 0$.

Lemma 4.1. *Equivalent valuations induce the same topology.*

Proof. If $|\cdot|_1 = |\cdot|_2^r$, then $|x-a|_1 < d$ if and only if $|x-a|_2^r < d$ if and only if $|x-a|_2 < d^{1/r}$ so $B_1(a,d) = B_2(a, d^{1/r})$. Thus the basis of open neighborhoods of a for $|\cdot|_1$ and $|\cdot|_2$ are identical. $\square$

A valuation satisfying the triangle inequality gives a metric for the topology on defining the distance from a to b to be $|a-b|$. Assume for the rest of this section that we only consider valuations that satisfy the triangle inequality.

Lemma 4.2. *A field with the topology induced by a valuation is a topological field, i.e., the operations sum, product, and reciprocal are continuous.*

Proof. For example (product) the triangle inequality implies that

$$|(a+\varepsilon)(b+\delta) - ab| \le |\varepsilon|\,|\delta| + |a|\,|\delta| + |b|\,|\varepsilon|$$

is small when $|\varepsilon|$ and $|\delta|$ are small (for fixed a, b). $\square$

Lemma 4.3. *Suppose two valuations $|\cdot|_1$ and $|\cdot|_2$ on the same field K induce the same topology. Then for any sequence $\{x_n\}$ in K we have*

$$|x_n|_1 \to 0 \iff |x_n|_2 \to 0.$$

Proof. It suffices to prove that if $|x_n|_1 \to 0$ then $|x_n|_2 \to 0$, since the proof of the other implication is the same. Let $\varepsilon > 0$. The topologies induced by the two absolute values are the same, so $B_2(0, \varepsilon)$ can be covered by open balls $B_1(a_i, r_i)$. One of these open balls $B_1(a, r)$ contains 0. There is $\varepsilon' > 0$ such that

$$B_1(0, \varepsilon') \subset B_1(a, r) \subset B_2(0, \varepsilon).$$

Since $|x_n|_1 \to 0$, there exists N such that for $n \ge N$ we have $|x_n|_1 < \varepsilon'$. For such n, we have $x_n \in B_1(0, \varepsilon')$, so $x_n \in B_2(0, \varepsilon)$, so $|x_n|_2 < \varepsilon$. Thus $|x_n|_2 \to 0$. $\square$

Proposition 4.4. *If two valuations $|\cdot|_1$ and $|\cdot|_2$ on the same field induce the same topology, then they are equivalent in the sense that there is a positive real α such that $|\cdot|_1 = |\cdot|_2^\alpha$.*

Proof. If $x \in K$ and $i = 1, 2$, then $|x^n|_i \to 0$ if and only if $|x|_i^n \to 0$, which is the case if and only if $|x|_i < 1$. Thus Lemma 4.3 implies that $|x|_1 < 1$ if and only if $|x|_2 < 1$. On taking reciprocals we see that $|x|_1 > 1$ if and only if $|x|_2 > 1$, so finally $|x|_1 = 1$ if and only if $|x|_2 = 1$.

Let now $w, z \in K$ be nonzero elements with $|w|_i \ne 1$ and $|z|_i \ne 1$. On applying the foregoing to

$$x = w^m z^n \qquad (m, n \in \mathbf{Z})$$

we see that

$$m \log |w|_1 + n \log |z|_1 \ge 0$$

if and only if

$$m \log |w|_2 + n \log |z|_2 \ge 0.$$

Dividing through by $\log |z|_i$, and rearranging, we see that for every rational number $\alpha = -n/m$,

$$\frac{\log |w|_1}{\log |z|_1} \ge \alpha \iff \frac{\log |w|_2}{\log |z|_2} \ge \alpha.$$

Thus

$$\frac{\log |w|_1}{\log |z|_1} = \frac{\log |w|_2}{\log |z|_2},$$

so

$$\frac{\log |w|_1}{\log |w|_2} = \frac{\log |z|_1}{\log |z|_2}.$$

Since this equality does not depend on the choice of z, we see that there is a constant c ($= \log |z|_1 / \log |z|_2$) such that $\log |w|_1 / \log |w|_2 = c$ for all w. Thus $\log |w|_1 = c \cdot \log |w|_2$, so $|w|_1 = |w|_2^c$, which implies that $|\cdot|_1$ is equivalent to $|\cdot|_2$. $\square$

5 Completeness

We recall the definition of metric on a set X.

Definition 5.1 (Metric). A *metric* on a set X is a map

$$d : X \times X \to \mathbf{R}$$

such that for all $x, y, z \in X$,

1. $d(x, y) \geq 0$ and $d(x, y) = 0$ if and only if $x = y$,
2. $d(x, y) = d(y, x)$, and
3. $d(x, z) \leq d(x, y) + d(y, z)$.

A *Cauchy sequence* is a sequence (x_n) in X such that for all $\varepsilon > 0$ there exists M such that for all $n, m > M$ we have $d(x_n, x_m) < \varepsilon$. The *completion* of X is the set of Cauchy sequences (x_n) in X modulo the equivalence relation in which two Cauchy sequences (x_n) and (y_n) are equivalent if $\lim_{n\to\infty} d(x_n, y_n) = 0$. A metric space is *complete* if every Cauchy sequence converges, and one can show that the completion of X with respect to a metric is complete.

For example, $d(x, y) = |x - y|$ (usual archimedean absolute value) defines a metric on $\mathbf{Q}$. The completion of $\mathbf{Q}$ with respect to this metric is the field $\mathbf{R}$ of real numbers. More generally, whenever $|\cdot|$ is a valuation on a field K that satisfies the triangle inequality, then $d(x, y) = |x - y|$ defines a metric on K. Consider for the rest of this section only valuations that satisfy the triangle inequality.

Definition 5.2 (Complete). A field K is *complete* with respect to a valuation $|\cdot|$ if given any Cauchy sequence a_n, ($n = 1, 2, \ldots$), i.e., one for which

$$|a_m - a_n| \to 0 \qquad (m, n \to \infty, \infty),$$

there is an $a^* \in K$ such that

$$a_n \to a^* \qquad \text{w.r.t. } |\cdot|$$

(i.e., $|a_n - a^*| \to 0$).

Theorem 5.3. *Every field K with valuation $v = |\cdot|$ can be embedded in a complete field K_v with a valuation $|\cdot|$ extending the original one in such a way that K_v is the closure of K with respect to $|\cdot|$. Further K_v is unique up to a unique isomorphism fixing K.*

Proof. Define K_v to be the completion of K with respect to the metric defined by $|\cdot|$. Thus K_v is the set of equivalence classes of Cauchy sequences, and there is a natural injective map from K to K_v sending an element $a \in K$ to the constant Cauchy sequence (a). Because the field operations on K are continuous, they induce well-defined field operations on equivalence classes of Cauchy sequences componentwise. Also, define a valuation on K_v by

$$|(a_n)_{n=1}^{\infty}| = \lim_{n\to\infty} |a_n| \,,$$

and note that this is well defined and extends the valuation on K.

To see that K_v is unique up to a unique isomorphism fixing K, we observe that there are no nontrivial continuous automorphisms $K_v \to K_v$ that fix K. This is because, by denseness, a continuous automorphism $\sigma : K_v \to K_v$ is determined by what it does to K, and by assumption σ is the identity map on K. More precisely, suppose $a \in K_v$ and n is a positive integer. Then by continuity there is $\delta > 0$ (with $\delta < 1/n$) such that if $a_n \in K_v$ and $|a - a_n| < \delta$ then $|\sigma(a) - \sigma(a_n)| < 1/n$. Since K is dense in K_v, we can choose the a_n above to be an element of K. Then by hypothesis $\sigma(a_n) = a_n$, so $|\sigma(a) - a_n| < 1/n$. Thus $\sigma(a) = \lim_{n\to\infty} a_n = a$. $\square$

Corollary 5.4. *The valuation $|\cdot|$ is non-archimedean on K_v if and only if it is so on K. If $|\cdot|$ is non-archimedean, then the set of values taken by $|\cdot|$ on K and K_v are the same.*

Proof. The first part follows from the fact proved earlier that a valuation is non-archimedean if and only if $|n| < 1$ for all integers n. Since the valuation on K_v extends the valuation on K, and all n are in K, the first statement follows.

For the second, suppose that $|\cdot|$ is non-archimedean (but not necessarily discrete). Suppose $b \in K_v$ with $b \neq 0$. First I claim that there is $c \in K$ such that $|b - c| < |b|$. To see this, let $c' = b - \frac{b}{a}$, where a is some element of K_v with $|a| > 1$, note that $|b - c'| = \left|\frac{b}{a}\right| < |b|$, and choose $c \in K$ such that $|c - c'| < |b - c'|$, so

$$|b - c| = \left|b - c' - (c - c')\right| \leq \max\left(\left|b - c'\right|, \left|c - c'\right|\right) = \left|b - c'\right| < |b| \,.$$

Since $|\cdot|$ is non-archimedean, we have

$$|b| = |(b - c) + c| \leq \max\left(|b - c|, |c|\right) = |c| \,,$$

where in the last equality we use that $|b - c| < |b|$. Also,

$$|c| = |b + (c - b)| \leq \max\left(|b|, |c - b|\right) = |b| \,,$$

so $|b| = |c|$, which is in the set of values of $|\cdot|$ on K. $\square$

5.1 p-adic Numbers

This section is about the p-adic numbers $\mathbf{Q}_p$, which are the completion of $\mathbf{Q}$ with respect to the p-adic valuation. Alternatively, to give a p-adic *integer* in $\mathbf{Z}_p$ is the same as giving for every prime power p^r an element $a_r \in \mathbf{Z}/p^r\mathbf{Z}$ such that if $s \leq r$ then a_s is the reduction of a_r modulo p^s. The field $\mathbf{Q}_p$ is then the field of fractions of $\mathbf{Z}_p$.

We begin with the definition of the N-adic numbers for any positive integer N. Section 5.1.2 is about the N-adics in the special case $N = 10$; these are fun because they can be represented as decimal expansions that go off infinitely far to the left. Section 5.3 is about how the topology of $\mathbf{Q}_N$ is nothing like the topology of $\mathbf{R}$. Finally, in Section 5.4 we state the Hasse-Minkowski theorem, which shows how to use p-adic numbers to decide whether or not a quadratic equation in n variables has a rational zero.

5.1.1 The N-adic Numbers

Lemma 5.5. *Let N be a positive integer. Then for any nonzero rational number α there exists a unique $e \in \mathbf{Z}$ and integers a, b, with b positive, such that $\alpha = N^e \cdot \frac{a}{b}$ with $N \nmid a$, $\gcd(a, b) = 1$, and $\gcd(N, b) = 1$.*

Proof. Write $\alpha = c/d$ with $c, d \in \mathbf{Z}$ and $d > 0$. First suppose d is exactly divisible by a power of N, so for some r we have $N^r \mid d$ but $\gcd(N, d/N^r) = 1$. Then

$$\frac{c}{d} = N^{-r}\frac{c}{d/N^r}.$$

If N^s is the largest power of N that divides c, then $e = s - r$, $a = c/N^s$, $b = d/N^r$ satisfy the conclusion of the lemma.

By unique factorization of integers, there is a smallest multiple f of d such that fd is exactly divisible by N. Now apply the above argument with c and d replaced by cf and df. $\square$

Definition 5.6 (N-adic valuation). Let N be a positive integer. For any positive $\alpha \in \mathbf{Q}$, the *N-adic valuation* of α is e, where e is as in Lemma 5.5. The N-adic valuation of 0 is ∞.

We denote the N-adic valuation of α by $\mathrm{ord}_N(\alpha)$. (Note: Here we are using "valuation" in a different way than in the rest of the text. This valuation is not an absolute value, but the logarithm of one.)

Definition 5.7 (N-adic metric). For $x, y \in \mathbf{Q}$ the *N-adic distance* between x and y is

$$d_N(x, y) = N^{-\mathrm{ord}_N(x-y)}.$$

We let $d_N(x, x) = 0$, since $\mathrm{ord}_N(x - x) = \mathrm{ord}_N(0) = \infty$.

For example, $x, y \in \mathbf{Z}$ are close in the N-adic metric if their difference is divisible by a large power of N. E.g., if $N = 10$ then 93427 and 13427 are close because their difference is 80000, which is divisible by a large power of 10.

Proposition 5.8. *The distance d_N on $\mathbf{Q}$ defined above is a metric. Moreover, for all $x, y, z \in \mathbf{Q}$ we have*

$$d(x, z) \leq \max(d(x, y), d(y, z)).$$

(This is the "nonarchimedean" triangle inequality.)

Proof. The first two properties of Definition 5.1 are immediate. For the third, we first prove that if $\alpha, \beta \in \mathbf{Q}$ then

$$\mathrm{ord}_N(\alpha + \beta) \geq \min(\mathrm{ord}_N(\alpha), \mathrm{ord}_N(\beta)).$$

Assume, without loss, that $\mathrm{ord}_N(\alpha) \leq \mathrm{ord}_N(\beta)$ and that both α and β are nonzero. Using Lemma 5.5 write $\alpha = N^e(a/b)$ and $\beta = N^f(c/d)$ with a or c possibly negative. Then

$$\alpha + \beta = N^e\left(\frac{a}{b} + N^{f-e}\frac{c}{d}\right) = N^e\left(\frac{ad + bcN^{f-e}}{bd}\right).$$

Since $\gcd(N, bd) = 1$ it follows that $\mathrm{ord}_N(\alpha + \beta) \geq e$. Now suppose $x, y, z \in \mathbf{Q}$. Then

$$x - z = (x - y) + (y - z),$$

so

$$\mathrm{ord}_N(x - z) \geq \min(\mathrm{ord}_N(x - y), \mathrm{ord}_N(y - z)),$$

hence $d_N(x, z) \leq \max(d_N(x, y), d_N(y, z))$. $\square$

We can finally define the N-adic numbers.

Definition 5.9 (The N-adic Numbers). The set of *N-adic numbers*, denoted $\mathbf{Q}_N$, is the completion of $\mathbf{Q}$ with respect to the metric d_N.

The set $\mathbf{Q}_N$ is a ring, but it need not be a field as you will show in Exercises 4 and 5. It is a field if and only if N is prime. Also, $\mathbf{Q}_N$ has a "bizarre" topology, as we will see in Section 5.3.

5.1.2 The 10-adic Numbers

It's a familiar fact that every real number can be written in the form

$$d_n \dots d_1 d_0 . d_{-1} d_{-2} \dots = d_n 10^n + \cdots + d_1 10 + d_0 + d_{-1} 10^{-1} + d_{-2} 10^{-2} + \cdots$$

where each digit d_i is between 0 and 9, and the sequence can continue indefinitely to the right.

The 10-adic numbers also have decimal expansions, but everything is backward! To get a feeling for why this might be the case, we consider Euler's nonsensical series

$$\sum_{n=1}^{\infty}(-1)^{n+1}n! = 1! - 2! + 3! - 4! + 5! - 6! + \cdots .$$

You will prove in Exercise 2 that this series converges in $\mathbf{Q}_{10}$ to some element $\alpha \in \mathbf{Q}_{10}$.

What is α? How can we write it down? First note that for all $M \geq 5$, the terms of the sum are divisible by 10, so the difference between α and $1! - 2! + 3! - 4!$ is divisible by 10. Thus we can compute α modulo 10 by computing $1! - 2! + 3! - 4!$ modulo 10. Likewise, we can compute α modulo 100 by compute $1! - 2! + \cdots + 9! - 10!$, etc. We obtain the following table:

α	mod 10^r
1	mod 10
81	mod 10^2
981	mod 10^3
2981	mod 10^4
22981	mod 10^5
422981	mod 10^6

Continuing we see that

$$1! - 2! + 3! - 4! + \cdots = \ldots 637838364422981 \qquad \text{in } \mathbf{Q}_{10}\ !$$

Here's another example. Reducing $1/7$ modulo larger and larger powers of 10 we see that

$$\frac{1}{7} = \ldots 857142857143 \qquad \text{in } \mathbf{Q}_{10}.$$

Here's another example, but with a decimal point.

$$\frac{1}{70} = \frac{1}{10} \cdot \frac{1}{7} = \ldots 85714285714.3$$

We have

$$\frac{1}{3} + \frac{1}{7} = \ldots 66667 + \ldots 57143 = \frac{10}{21} = \ldots 23810,$$

which illustrates that addition with carrying works as usual.

5.1.3 Fermat's Last Theorem in $\mathbf{Z}_{10}$

An amusing observation, which people often argued about on USENET news back in the 1990s, is that Fermat's last theorem is false in $\mathbf{Z}_{10}$. For example, $x^3 + y^3 = z^3$ has a nontrivial solution, namely $x = 1$, $y = 2$, and $z = \ldots 60569$. Here z is a cube root of 9 in $\mathbf{Z}_{10}$. Note that it takes some work to prove that there is a cube root of 9 in $\mathbf{Z}_{10}$ (see Exercise 3).

5.2 The Field of p-adic Numbers

The ring $\mathbf{Q}_{10}$ of 10-adic numbers is isomorphic to $\mathbf{Q}_2 \times \mathbf{Q}_5$ (see Exercise 5), so it is not a field. For example, the element $\ldots 8212890625$ corresponding to $(1, 0)$ under this isomorphism has no inverse. (To compute n digits of $(1, 0)$ use the Chinese remainder theorem to find a number that is 1 modulo 2^n and 0 modulo 5^n.)

If p is prime then $\mathbf{Q}_p$ is a field (see Exercise 4). Since $p \neq 10$ it is a little more complicated to write p-adic numbers down. People typically write p-adic numbers in the form

$$\frac{a_{-d}}{p^d} + \cdots + \frac{a_{-1}}{p} + a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \cdots$$

where $0 \leq a_i < p$ for each i.

5.3 The Topology of $\mathbf{Q}_N$ (is Weird)

Definition 5.10 (Connected). Let X be a topological space. A subset S of X is *disconnected* if there exist open subsets $U_1, U_2 \subset X$ with $U_1 \cap U_2 \cap S = \emptyset$ and $S = (S \cap U_1) \cup (S \cap U_2)$ with $S \cap U_1$ and $S \cap U_2$ nonempty. If S is not disconnected it is *connected*.

The topology on $\mathbf{Q}_N$ is induced by d_N, so every open set is a union of open balls

$$B(x, r) = \{y \in \mathbf{Q}_N : d_N(x, y) < r\}.$$

Recall Proposition 5.8, which asserts that for all x, y, z,

$$d(x, z) \leq \max(d(x, y), d(y, z)).$$

This translates into the following shocking and bizarre lemma:

Lemma 5.11. *Suppose $x \in \mathbf{Q}_N$ and $r > 0$. If $y \in \mathbf{Q}_N$ and $d_N(x, y) \geq r$, then $B(x, r) \cap B(y, r) = \emptyset$.*

Proof. Suppose $z \in B(x, r)$ and $z \in B(y, r)$. Then

$$r \leq d_N(x, y) \leq \max(d_N(x, z), d_N(z, y)) < r,$$

a contradiction. $\square$

You should draw a picture to illustrates Lemma 5.11.

Lemma 5.12. *The open ball $B(x, r)$ is also closed.*

Proof. Suppose $y \notin B(x, r)$. Then $r \leq d(x, y)$ so

$$B(y, d(x, y)) \cap B(x, r) \subset B(y, d(x, y)) \cap B(x, d(x, y)) = \emptyset.$$

Thus the complement of $B(x, r)$ is a union of open balls. $\square$

The lemmas imply that $\mathbf{Q}_N$ is *totally disconnected*, in the following sense.

Proposition 5.13. *The only connected subsets of $\mathbf{Q}_N$ are the singleton sets $\{x\}$ for $x \in \mathbf{Q}_N$ and the empty set.*

Proof. Suppose $S \subset \mathbf{Q}_N$ is a nonempty connected set and x, y are distinct elements of S. Let $r = d_N(x, y) > 0$. Let $U_1 = B(x, r)$ and U_2 be the complement of U_1, which is open by Lemma 5.12. Then U_1 and U_2 satisfies the conditions of Definition 5.10, so S is not connected, a contradiction. □

5.4 The Local-to-Global Principle of Hasse and Minkowski

Section 5.3 might have convinced you that $\mathbf{Q}_N$ is a bizarre pathology. In fact, $\mathbf{Q}_N$ is omnipresent in number theory, as the following two fundamental examples illustrate.

In the statement of the following theorem, a *nontrivial solution* to a homogeneous polynomial equation is a solution where not all indeterminates are 0.

Theorem 5.14 (Hasse-Minkowski). *The quadratic equation*

$$a_1 x_1^2 + a_2 x_2^2 + \cdots + a_n x_n^2 = 0, \tag{5.1}$$

with $a_i \in \mathbf{Q}^\times$, has a nontrivial solution with $x_1, \ldots, x_n$ in $\mathbf{Q}$ if and only if (5.1) has a solution in $\mathbf{R}$ and in $\mathbf{Q}_p$ for all primes p.

This theorem is very useful in practice because the p-adic condition turns out to be easy to check. For more details, including a complete proof, see [Serre, *A Course in Arithmetic*, IV.3.2]].

The analogue of Theorem 5.14 for cubic equations is false. For example, Selmer proved that the cubic

$$3x^3 + 4y^3 + 5z^3 = 0$$

has a solution other than $(0, 0, 0)$ in $\mathbf{R}$ and in $\mathbf{Q}_p$ for all primes p but has no solution other than $(0, 0, 0)$ in $\mathbf{Q}$ (for a proof see [Cassels, *Lectures on Elliptic Curves*, §18]).

Open Problem. Give an algorithm that decides whether or not a cubic

$$ax^3 + by^3 + cz^3 = 0$$

has a nontrivial solution in $\mathbf{Q}$.

This open problem is closely related to the Birch and Swinnerton-Dyer Conjecture for elliptic curves. The truth of the conjecture would follow if we knew that "Shafarevich-Tate Groups" of elliptic curves were finite.

5.5 Exercises

The following are *optional exercises*, which you may want to do if you would like to familiarize yourself further with p-adic numbers. They are not part of the formal homework sets and you do not need to hand them in.

1. Compute the first 5 digits of the 10-adic expansions of the following rational numbers:
$$\frac{13}{2}, \quad \frac{1}{389}, \quad \frac{17}{19}, \qquad \text{the 4 square roots of 41.}$$

2. Let $N > 1$ be an integer. Prove that the series
$$\sum_{n=1}^{\infty}(-1)^{n+1}n! = 1! - 2! + 3! - 4! + 5! - 6! + \cdots .$$
converges in $\mathbf{Q}_N$.

3. Prove that -9 has a cube root in $\mathbf{Q}_{10}$ using the following strategy (this is a special case of "Hensel's Lemma").

   (a) Show that there is $\alpha \in \mathbf{Z}$ such that $\alpha^3 \equiv 9 \pmod{10^3}$.

   (b) Suppose $n \geq 3$. Use induction to show that if $\alpha_1 \in \mathbf{Z}$ and $\alpha^3 \equiv 9 \pmod{10^n}$, then there exists $\alpha_2 \in \mathbf{Z}$ such that $\alpha_2^3 \equiv 9 \pmod{10^{n+1}}$. (Hint: Show that there is an integer b such that $(\alpha_1 + b10^n)^3 \equiv 9 \pmod{10^{n+1}}$.)

   (c) Conclude that 9 has a cube root in $\mathbf{Q}_{10}$.

4. Let $N > 1$ be an integer.

   (a) Prove that $\mathbf{Q}_N$ is equipped with a natural ring structure.

   (b) If N is prime, prove that $\mathbf{Q}_N$ is a field.

5. (a) Let p and q be distinct primes. Prove that $\mathbf{Q}_{pq} \cong \mathbf{Q}_p \times \mathbf{Q}_q$.

   (b) Is $\mathbf{Q}_{p^2}$ isomorphic to either of $\mathbf{Q}_p \times \mathbf{Q}_p$ or $\mathbf{Q}_p$?