Math 129: Algebraic Number Theory

Lecture 19: Normed Spaces and Tensor Products

William Stein

Tuesday, April 20, 2004

Much of today's lecture is preparation for what we will do next time, when we will prove that if K is complete with respect to a valuation (and locally compact) and L is a finite extension of K, then there is a *unique* valuation on L that extends the valuation on K. Also, if K is a number field, $v = |\cdot|$ is a valuation on K, K_v is the completion of K with respect to v, and L is a finite extension of K, we'll prove that

$$K_v \otimes_K L = \bigoplus_{j=1}^{J} L_j,$$

where the L_j are the completions of L with respect to the equivalence classes of extensions of v to L. In particular, if L is a number field defined by a root of $f(x) \in \mathbf{Q}[x]$, then

$$\mathbf{Q}_p \otimes_{\mathbf{Q}} L = \bigoplus_{j=1}^{J} L_j,$$

where the L_j correspond to the irreducible factors of the polynomial $f(x) \in \mathbf{Q}_p[x]$ (hence the extensions of $|\cdot|_p$ correspond to irreducible factors of $f(x)$ over $\mathbf{Q}_p[x]$).

In preparation for this clean view of the local nature of number fields, today we will prove that the norms on a finite-dimensional vector space over a complete field are all equivalent. We will also explicitly construct tensor products of fields and deduce some of their properties.

8 Normed Spaces

Definition 8.1 (Norm). Let K be a field with valuation $|\cdot|$ and let V be a vector space over K. A real-valued function $\|\cdot\|$ on V is called a norm if

1. $\|v\| > 0$ for all nonzero $v \in V$ (positivity).
2. $\|v + w\| \leq \|v\| + \|w\|$ for all $v, w \in V$ (triangle inequality).
3. $\|av\| = |a|\,\|v\|$ for all $a \in K$ and $v \in V$ (homogeneity).

Note that setting $\|v\| = 1$ for all $v \neq 0$ does *not* define a norm unless the absolute value on K is trivial, as $1 = \|av\| = |a|\,\|v\| = |a|$. We assume for the rest of this section that $|\cdot|$ is not trivial.

Definition 8.2 (Equivalent). Two norms $\|\cdot\|_1$ and $\|\cdot\|_2$ on the same vector space V are equivalent if there exists positive real numbers c_1 and c_2 such that for all $v \in V$

$$\|v\|_1 \leq c_1 \|v\|_2 \qquad \text{and} \qquad \|v\|_2 \leq c_2 \|v\|_1 .$$

Lemma 8.3. *Suppose that K is a field that is complete with respect to a valuation $|\cdot|$ and that V is a finite dimensional K vector space. Then any two norms on V are equivalent.*

Remark 8.4. As we shall see next time, the lemma is usually false if we do not assume that K is complete. For example, when $K = \mathbf{Q}$ and $|\cdot|_p$ is the p-adic valuation, and V is a number field, then there may be several extensions of $|\cdot|_p$ to inequivalent norms on V.

If two norms are equivalent then the corresponding topologies on V are equal, since very open ball for $\|\cdot\|_1$ is contained in an open ball for $\|\cdot\|_2$, and conversely. (The converse is also true, since, as we will show, all norms on V are equivalent.)

Proof. Let $v_1, \ldots, v_n$ be a basis for V. Define the max norm $\|\cdot\|_0$ by

$$\left\| \sum_{n=1}^{N} a_n v_n \right\|_0 = \max\left\{ |a_n| : n = 1, \ldots, N \right\} .$$

It is enough to show that any norm $\|\cdot\|$ is equivalent to $\|\cdot\|_0$. We have

$$\begin{aligned} \left\| \sum_{n=1}^{N} a_n v_n \right\| &\leq \sum_{n=1}^{N} |a_n|\, \|v_n\| \\ &\leq \sum_{n=1}^{N} \max |a_n|\, \|v_n\| \\ &= c_1 \cdot \left\| \sum_{n=1}^{N} a_n v_n \right\|_0 , \end{aligned}$$

where $c_1 = \sum_{n=1}^{N} \|v_n\|$.

To finish the proof, we show that there is a $c_2 \in \mathbf{R}$ such that for all $v \in V$,

$$\|v\|_0 \leq c_2 \cdot \|v\| .$$

We will only prove this in the case when K is not just merely complete with respect to $|\cdot|$ but also locally compact. This will be the case of primary interest to us. For a proof in the general case, see the original article by Cassels (page 53).

By what we have already shown, the function $\|v\|$ is continuous in the $\|\cdot\|_0$-topology, so by local compactness it attains its lower bound δ on the unit circle $\{v \in V : \|v\|_0 = 1\}$. (Why is the unit circle compact? With respect to $\|\cdot\|_0$, the topology on V is the same as that of a product of copies of K. If the valuation is archimedean then $K \cong \mathbf{R}$ or $\mathbf{C}$ with the standard topology and the unit circle is compact. If the valuation is non-archimedean, then we saw last time in a (at the time dubious) remark that if K is locally compact, then the valuation is discrete, in which case we showed that the unit disc is compact, hence the unit circle is also since it is closed.) Note that $\delta > 0$ by part 1 of Definition 8.1. Also, by definition of $\|\cdot\|_0$, for any $v \in V$ there exists $a \in K$ such that $\|v\|_0 = |a|$ (just take the max coefficient in our basis). Thus we can write any $v \in V$ as $a \cdot w$ where $a \in K$ and $w \in V$ with $\|w\|_0 = 1$. We then have

$$\frac{\|v\|_0}{\|v\|} = \frac{\|aw\|_0}{\|aw\|} = \frac{|a|\,\|w\|_0}{|a|\,\|w\|} = \frac{1}{\|w\|} \leq \frac{1}{\delta}.$$

Thus for all v we have

$$\|v\|_0 \leq c_2 \cdot \|v\|,$$

where $c_2 = 1/\delta$, which proves the theorem. □

9 Tensor Products

We need only a special case of the tensor product construction. Let A and B be commutative rings containing a field K and suppose that B is of finite dimension N over K, say, with basis

$$1 = w_1, w_2, \ldots, w_N.$$

Then B is determined up to isomorphism as a ring over K by the multiplication table $(c_{i,j,n})$ defined by

$$w_i \cdot w_j = \sum_{n=1}^{N} c_{i,j,n} \cdot w_n.$$

We define a new ring C containing K whose elements are the set of all expressions

$$\sum_{n=1}^{N} a_n \underline{w}_n$$

where the $\underline{w}_n$ have the same multiplication rule

$$\underline{w}_i \cdot \underline{w}_j = \sum_{n=1}^{N} c_{i,j,n} \cdot \underline{w}_n$$

as the w_n.

There are injective ring homomorphisms

$$i : A \hookrightarrow C, \qquad i(a) = a\underline{w}_1 \qquad (\text{note that } \underline{w}_1 = 1)$$

and

$$j : B \hookrightarrow C, \qquad j\left(\sum_{n=1}^{N} c_n w_n\right) = \sum_{n=1}^{N} c_n \underline{w}_n.$$

Moreover C is defined, up to isomorphism, by A and B and is independent of the particular choice of basis w_n of B (i.e., a change of basis of B induces a canonical isomorphism of the C defined by the first basis to the C defined by the second basis). We write

$$C = A \otimes_K B$$

since C is, in fact, a special case of the ring tensor product. (This will be one of your homework problems.)

Let us now suppose, further, that A is a topological ring, i.e., has a topology with respect to which addition and multiplication are continuous. Then the map

$$C \to A \oplus \cdots \oplus A, \qquad \sum_{m=1}^{N} a_m \underline{w}_m \mapsto (a_1, \ldots, a_N)$$

defines a bijection between C and the product of N copies of A (considered as sets). We give C the product topology. It is readily verified that this topology is independent of the choice of basis $w_1, \ldots, w_N$ and that multiplication and addition on C are continuous, so C is a topological ring. We call this topology on C the *tensor product topology.*

Now drop our assumption that A and B have a topology, but suppose that A and B are not merely rings but fields. Recall that a finite extension L/K of fields is *separable* if the number of embeddings $L \hookrightarrow \overline{K}$ that fix K equals the degree of L over K, where $\overline{K}$ is an algebraic closure of K. The primitive element theorem from Galois theory asserts that any such extension is generated by a single element, i.e., $L = K(a)$ for some $a \in L$.

Lemma 9.1. *Let A and B be fields containing the field K and suppose that B is a separable extension of finite degree $N = [B : K]$. Then $C = A \otimes_K B$ is the direct sum of a finite number of fields K_j, each containing an isomorphic image of A and an isomorphic image of B.*

Proof. By the primitive element theorem, we have $B = K(b)$, where b is a root of some separable irreducible polynomial $f(x) \in K[x]$ of degree N. Then $1, b, \ldots, b^{N-1}$ is a basis for B over K, so

$$A \otimes_K B = A[\underline{b}] \cong A[x]/(f(x))$$

where $1, \underline{b}, \underline{b}^2, \ldots, \underline{b}^{N-1}$ are linearly independent over A and $\underline{b}$ satisfies $f(\underline{b}) = 0$.

Although the polynomial $f(x)$ is irreducible as an element of $K[x]$, it need not be irreducible in $A[x]$. Since A is a field, we have a factorization

$$f(x) = \prod_{j=1}^{J} g_j(x)$$

where $g_j(x) \in A[x]$ is irreducible. The $g_j(x)$ are distinct because $f(x)$ is separable (i.e., has distinct roots in any algebraic closure).

For each j, let $\underline{b}_j \in \overline{A}$ be a root of $g_j(x)$, where $\overline{A}$ is a fixed algebraic closure of the field A. Let $K_j = A(\underline{b}_j)$. Then the map

$$\varphi_j : A \otimes_K B \to K_j \tag{9.1}$$

given by sending any polynomial $h(\underline{b})$ in $\underline{b}$ (where $h \in A[x]$) to $h(\underline{b}_j)$ is a ring homomorphism, because the image of $\underline{b}$ satisfies the polynomial $f(x)$, and $A \otimes_K B \cong A[x]/(f(x))$.

By the Chinese Remainder Theorem, the maps from (9.1) combine to define a ring isomorphism

$$A \otimes_K B \cong A[x]/(f(x)) \cong \bigoplus_{j=1}^{J} A[x]/(g_j(x)) \cong \bigoplus_{j=1}^{J} K_j.$$

Each K_j is of the form $A[x]/(g_j(x))$, so contains an isomorphic image of A. It thus remains to show that the ring homomorphisms

$$\lambda_j : B \xrightarrow{b \mapsto 1 \otimes b} A \otimes_K B \xrightarrow{\varphi_j} K_j$$

are injections. Since B and K_j are both fields, λ_j is either the 0 map or injective. However, λ_j is not the 0 map since $\lambda_j(1) = 1 \in K_j$. □

Example 9.2. If A and B are finite extensions of $\mathbf{Q}$, then $A \otimes_{\mathbf{Q}} B$ is an algebra of degree $[A : \mathbf{Q}] \cdot [B : \mathbf{Q}]$. For example, suppose A is generated by a root of $x^2 + 1$ and B is generated by a root of $x^3 - 2$. We can view $A \otimes_{\mathbf{Q}} B$ as either $A[x]/(x^3 - 2)$ or $B[x]/(x^2 + 1)$. The polynomial $x^2 + 1$ is irreducible over $\mathbf{Q}$, and if it factored over the cubic field B, then there would be a root of $x^2 + 1$ in B, i.e., the quadratic field $A = \mathbf{Q}(i)$ would be a subfield of the cubic field $B = \mathbf{Q}(\sqrt[3]{2})$, which is impossible. Thus $x^2 + 1$ is irreducible over B, so $A \otimes_{\mathbf{Q}} B = A.B = \mathbf{Q}(i, \sqrt[3]{2})$ is a degree 6 extension of $\mathbf{Q}$. Notice that $A.B$ contains a copy A and a copy of B. By the primitive element theorem the composite field $A.B$ can be generated by the root of a single polynomial. For example, the minimal polynomial of $i + \sqrt[3]{2}$ is $x^6 + 3x^4 - 4x^3 + 3x^2 + 12x + 5$, hence $\mathbf{Q}(i + \sqrt[3]{2}) = A.B$.

Example 9.3. The case $A \cong B$ is even more exciting. For example, suppose $A = B = \mathbf{Q}(i)$. Using the Chinese Remainder Theorem we have that

$$\mathbf{Q}(i) \otimes_{\mathbf{Q}} \mathbf{Q}(i) \cong \mathbf{Q}(i)[x]/(x^2 + 1) \cong \mathbf{Q}(i)[x]/((x - i)(x + i)) \cong \mathbf{Q}(i) \oplus \mathbf{Q}(i),$$

since $(x - i)$ and $(x + i)$ are coprime. The last isomorphism sends $a + bx$, with $a, b \in \mathbf{Q}(i)$, to $(a + bi, a - bi)$. Since $\mathbf{Q}(i) \oplus \mathbf{Q}(i)$ has zero divisors, the tensor product $\mathbf{Q}(i) \otimes_{\mathbf{Q}} \mathbf{Q}(i)$ must also have zero divisors. For example, $(1, 0)$ and $(0, 1)$ is a zero divisor pair on the right hand side, and we can trace back to the elements of the tensor product that they define. First, by solving the system

$$a + bi = 1 \qquad \text{and} \qquad a - bi = 0$$

we see that $(1, 0)$ corresponds to $a = 1/2$ and $b = -i/2$, i.e., to the element

$$\frac{1}{2} - \frac{i}{2}x \in \mathbf{Q}(i)[x]/(x^2 + 1).$$

This element in turn corresponds to

$$\frac{1}{2} \otimes 1 - \frac{i}{2} \otimes i \in \mathbf{Q}(i) \otimes_{\mathbf{Q}} \mathbf{Q}(i).$$

Similarly the other element $(0, 1)$ corresponds to

$$\frac{1}{2} \otimes 1 + \frac{i}{2} \otimes i \in \mathbf{Q}(i) \otimes_{\mathbf{Q}} \mathbf{Q}(i).$$

As a double check, observe that

$$\begin{aligned}\left(\frac{1}{2} \otimes 1 - \frac{i}{2} \otimes i\right) \cdot \left(\frac{1}{2} \otimes 1 + \frac{i}{2} \otimes i\right) &= \frac{1}{4} \otimes 1 + \frac{i}{4} \otimes i - \frac{i}{4} \otimes i - \frac{i^2}{4} \otimes i^2 \\ &= \frac{1}{4} \otimes 1 - \frac{1}{4} \otimes 1 = 0 \in \mathbf{Q}(i) \otimes_{\mathbf{Q}} \mathbf{Q}(i).\end{aligned}$$

Clearing the denominator of 2 and writing $1 \otimes 1 = 1$, we have $(1 - i \otimes i)(1 + i \otimes i) = 0$, so $i \otimes i$ is a root of the polynomimal $x^2 - 1$, and $i \otimes i$ is not ± 1, so $x^2 - 1$ has more than 2 roots.

In general, to understand $A \otimes_K B$ explicitly is the same as factoring either the defining polynomial of B over the field A, or factoring the defining polynomial of A over B.

Corollary 9.4. *Let $a \in B$ be any element and let $f(x) \in K[x]$ be the characteristic polynomials of a over K and let $g_j(x) \in A[x]$ (for $1 \leq j \leq J$) be the characteristic polynomials of the images of a under $B \to A \otimes_K B \to K_j$ over A, respectively. Then*

$$f(x) = \prod_{j=1}^{J} g_j(X). \tag{9.2}$$

Proof. We show that both sides of (9.2) are the characteristic polynomial $T(x)$ of the image of a in $A \otimes_K B$ over A. That $f(x) = T(x)$ follows at once by computing the characteristic polynomial in terms of a basis $\underline{w}_1, \ldots, \underline{w}_N$ of $A \otimes_K B$, where $w_1, \ldots, w_N$ is a basis for B over K (this is because the matrix of left multiplication by b on $A \otimes_K B$ is exactly the same as the matrix of left multiplication on B, so the characteristic polynomial doesn't change). To see that $T(X) = \prod g_j(X)$, compute the action of the image of a in $A \otimes_K B$ with respect to a basis of

$$A \otimes_K B \cong \bigoplus_{j=1}^{J} K_j \tag{9.3}$$

composed of basis of the individual extensions K_j of A. The resulting matrix will be a block direct sum of submatrices, each of whose characteristic polynomials is one of the $g_j(X)$. Taking the product gives the claimed identity (9.2). □

Corollary 9.5. *For $a \in B$ we have*

$$\mathrm{Norm}_{B/K}(a) = \prod_{j=1}^{J} \mathrm{Norm}_{K_j/A}(a),$$

and

$$\mathrm{Tr}_{B/K}(a) = \sum_{j=1}^{J} \mathrm{Tr}_{K_j/A}(a),$$

Proof. This follows from Corollary 9.4. First, the norm is ± the constant term of the characteristic polynomial, and the constant term of the product of polynomials is the product of the constant terms (and one sees that the sign matches up correctly). Second, the trace is minus the second coefficient of the characteristic polynomial, and second coefficients add when one multiplies polynomials:

$$(x^n + a_{n-1}x^{n-1} + \cdots) \cdot (x^m + a_{m-1}x^{m-1} + \cdots) = x^{n+m} + x^{n+m-1}(a_{m-1} + a_{n-1}) + \cdots .$$

One could also see both the statements by considering a matrix of left multiplication by a first with respect to the basis of $\underline{w}_n$ and second with respect to the basis coming from the left side of (9.3).

□