

Computing with real tori

Bill Casselman

In the representation theory of real reductive groups the algebraic tori contained in them and defined over \mathbb{R} play an extremely important part. This is very evident in, among other places, Fokko du Cloux's program *Atlas*, in which he deals continually with tori. In this short note I'll give a self-contained account of what seems to be going on, including a reasonably practical sketch of how to make computations; make some brief comments on the relevant code in *Atlas*; and then give some indication of some of the role the main result plays in representation theory. I also include in the section on implementation a remark of Kottwitz that describes easily the component group of any real torus.

1. Galois descent. If k is any field, the multiplicative group \mathbb{G}_m defined over k is the algebraic subvariety $xy - 1 = 0$ in two-dimensional affine space, with the natural group structure. For any extension ℓ/k , the group of its ℓ -rational points may be identified with ℓ^\times via projection onto the first coordinate axis.

An algebraic torus defined over k is an algebraic group defined over k that becomes isomorphic to a product of copies of \mathbb{G}_m over some finite extension of k . Over \mathbb{C} , all algebraic tori are in fact isomorphic to a product of copies of \mathbb{G}_m . We shall see that there is also a very simple classification for tori defined over \mathbb{R} .

If T is a torus defined over \mathbb{C} , let $X^*(T)$ be its **character lattice**, that of its algebraic homomorphisms into \mathbb{G}_m . If $T = (\mathbb{G}_m)^n$ then any one of these characters is of the form $(x_i) \mapsto \prod x_i^{n_i}$, so this group is isomorphic to \mathbb{Z}^n . In particular, it is always a free module over \mathbb{Z} of finite rank. The torus T may be recovered completely from X^* . If t lies in $T(\mathbb{C})$ then it gives rise to a map from X^* to \mathbb{C}^\times , $\chi \mapsto \chi(t)$. Using coordinates, one can see that this induces a canonical identification

$$T(\mathbb{C}) = \text{Hom}(X^*, \mathbb{C}^\times).$$

The **cocharacter lattice** of T is

$$X_*(T) = \text{Hom}_{\text{alg}}(\mathbb{G}_m, T).$$

Since all algebraic homomorphisms from \mathbb{G}_m to itself are of the form $x \mapsto x^n$, this is canonically isomorphic to the lattice dual to $X^*(T)$. The value of $\langle \mu, \lambda^\vee \rangle$ is characterized by the equation

$$\mu(\lambda^\vee(x)) = x^{\langle \mu, \lambda^\vee \rangle}$$

for all

$$\mu: T \rightarrow \mathbb{G}_m, \quad \lambda^\vee: \mathbb{G}_m \rightarrow T.$$

If $T = \mathbb{G}_m$, then its characters are algebraic functions on it, and its affine coordinate ring is $\mathbb{C}[x, x^{-1}]$, the ring generated by its characters. Similarly, the affine ring of any torus T may be identified with the group ring $\mathbb{C}[X^*(T)]$. That of $(\mathbb{G}_m)^n$, for example, is $\mathbb{C}[x_i^{\pm 1}]$.

Now suppose T to be a torus defined over \mathbb{R} . Conjugation acts on $T(\mathbb{C})$, and the group of real points is the subgroup of $T(\mathbb{C})$ fixed by it. Conjugation is also defined on $X^*(T)$:

$$\overline{\chi}(t) = \overline{\chi(\overline{t})}.$$

That is to say, the characters defined over \mathbb{R} are those satisfying

$$\chi(\overline{t}) = \overline{\chi(t)}.$$

For example, if T is \mathbb{G}_m or a product of copies of it, then this Galois action is trivial, since the characters $x \mapsto x^n$ are all defined already over \mathbb{R} .

Let's look at two more interesting examples.

(1) Suppose T to be the group \mathbb{S} of complex numbers of norm 1, which as a group defined over \mathbb{R} is the algebraic variety

$$c^2 + s^2 = 1.$$

Why is this a torus? Because over \mathbb{C} its equation factors as

$$(c + is)(c - is) = 1$$

which is the equation defining \mathbb{G}_m . That is to say, over \mathbb{C} we have an isomorphism between the (c, s) such that $c^2 + s^2 = 1$ and \mathbb{C}^\times , the map $z: (c, s) \mapsto c + is$. This generates the characters. Conjugation takes (c, s) to (\bar{c}, \bar{s}) , so the conjugate of z is

$$\overline{(c + is)} = c - is$$

which is z^{-1} . The conjugation action on $X^*(T)$ is therefore multiplication by -1 . Consistently with this the group of real points of the torus may be identified with the z such that $\bar{z}^{-1} = z$. The complex affine ring is $\mathbb{C}[z, z^{-1}]$ and the subring of conjugation invariants is generated by

$$c = \frac{z + z^{-1}}{2}, \quad s = \frac{z - z^{-1}}{2i}$$

which satisfy $c^2 + s^2 = 1$, sure enough.

(2) There is a torus defined over \mathbb{R} whose group of real points may be identified with \mathbb{C}^\times , which we may consider to be the complement in \mathbb{R}^2 of the origin, or the closed algebraic variety $(x^2 + y^2)z = 1$ in \mathbb{R}^3 . This becomes isomorphic to $\mathbb{C}^\times \times \mathbb{C}^\times$ over \mathbb{C} via the map $(x, y, z) \mapsto (x + iy, x - iy)$. Conjugation in $X^*(T) = \mathbb{Z}^2$ swaps the two coordinates. Here, the group of real points of the torus may be identified with the group of (w, z) such that $(\bar{z}, \bar{w}) = (w, z)$, or that of all (z, \bar{z}) .

In summary, every torus defined over \mathbb{R} gives rise to a free \mathbb{Z} -module of finite rank, namely its character group, and also an involution on it arising from the Galois action. Conversely, suppose we are given a free \mathbb{Z} -module L of finite rank, and suppose τ to be an involution of L . Then τ acts also as a kind of conjugation on the affine ring $\mathbb{C}[L]$:

$$\tau: \sum c_\lambda \lambda \mapsto \sum \bar{c}_\lambda \lambda^\tau.$$

The ring fixed by this is the real affine ring of a unique algebraic torus defined over \mathbb{R} .

In short:

[1] Proposition. (Classification by Galois descent) *Algebraic tori defined over \mathbb{R} are classified completely by involutions on free \mathbb{Z} -modules of finite rank.*

2. The classification. We have seen three different real tori so far: (1) the real multiplicative group itself, whose group of real points is the same as \mathbb{R}^\times ; (2) the complex unit group \mathbb{S} , whose real points are those on the unit circle $x^2 + y^2 = 1$; (3) what is called the restriction of the complex multiplicative group to \mathbb{R} , whose group of real points is \mathbb{C}^\times . There is a close relationship between these three tori, since we have a short exact sequence (written with some small abuse of language)

$$0 \longrightarrow X_*(\mathbb{S}) \longrightarrow X_*(\mathbb{C}^\times) \longrightarrow X_*(\mathbb{R}^\times) \longrightarrow 0,$$

equivalent to

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}^2 \longrightarrow \mathbb{Z} \longrightarrow 0.$$

Here the first non-trivial map takes m to $(m, -m)$, the second takes (m, n) to $m + n$.

I learned the following from Fokko du Cloux, although it is in some sense well known as part of the K -theory of the group of order two. Since it plays an important role in du Cloux's programs, I'll give a completely constructive proof.

[2] Theorem. *Every real algebraic torus is isomorphic to a product of copies of the three tori described above.*

In particular, its group of real points is isomorphic to a product of copies of \mathbb{R}^\times , \mathbb{C}^\times , and \mathbb{S} .

By the discussion in the last section, in order to prove the theorem it suffices to prove that if L is a free \mathbb{Z} -module of finite rank and τ an involution of L , then L may be decomposed

$$L = L_+ \oplus L_- \oplus L_{\text{sw}}$$

where $\tau = 1$ on L_+ , -1 on L_- , and a sum of two-dimensional swaps on L_{sw} . Explaining how to find this decomposition will require some computations on lattices. I'll explain the tools needed for this purpose in the next section, even though they are well known (found for example in [Pohst-Zassenhaus:1989]), and then in the one after that give the proof of the Theorem.

Incidentally, the decomposition is not canonical, as a simple example that I'll introduce later on will show. This does not matter in applications.

3. Lattice arithmetic. There are several lattice computations necessary to prove the Theorem constructively. The first result we'll need is a basic tool that will be used several times:

[3] Lemma. (Euclidean algorithm) *Given an integral vector $v = [v_1 \dots v_n]$, one can find an invertible integral matrix A such that*

$$vA = [0 \ 0 \ \dots \ d]$$

where d is (necessarily) the greatest common divisor of the coordinates of v .

Proof. The case $n = 1$ is trivial. Let's look next at the case $n = 2$. Given the vector $[m, n]$, we carry out the Euclidean algorithm to find the greatest common divisor d of m and n , keeping track of a few extra things as we go.

Precisely, we start with the vector $[m_0, n_0] = [m, n]$ and the matrix $A_0 = I$, the 2×2 identity. We are going to calculate a sequence of vectors and matrices $[m_i, n_i]$ and A_i , satisfying at all times the equation $[m_0, n_0]A_i = [m_i, n_i]$, and winding up with some $[m_i, n_i] = [0, d]$. As long as $m_i \neq 0$, in going from i to $i + 1$ we divide n_i by m_i :

$$\begin{aligned} n_i &= qm_i + r \\ n_{i+1} &= m_i \\ m_{i+1} &= r \\ A_{i+1} &= A_i \begin{bmatrix} -q & 1 \\ 1 & 0 \end{bmatrix} \end{aligned}$$

This works since

$$[m_{i+1} \ n_{i+1}] = [(n_i - qm_i) \ m_i] = [m_i \ n_i] \begin{bmatrix} -q & 1 \\ 1 & 0 \end{bmatrix} = [m_0 \ n_0]A_i \begin{bmatrix} -q & 1 \\ 1 & 0 \end{bmatrix}.$$

The process stops when division is exact and hence $r = 0$.

Now we continue by induction. We start with

$$v = [v_1 \ v_2 \ \dots \ v_n].$$

We may assume we have found an $(n - 1) \times (n - 1)$ A_{n-1} matrix embedded into an $n \times n$ matrix such that

$$v \begin{bmatrix} A_{n-1} & 0 \\ 0 & 1 \end{bmatrix} = [0 \ 0 \ \dots \ d_{n-1} \ v_n]$$

where d_{n-1} is the gcd of the first $n - 1$ coordinates of v . But then according to the case $n = 2$ we can multiply by an embedded 2×2 matrix to get $[0 \ 0 \ \dots \ d_n]$. qed

[4] Lemma. (Subspace saturation) *If U is a rational vector subspace of \mathbb{Q}^n then the intersection $U \cap \mathbb{Z}^n$ is a summand of \mathbb{Z}^n .*

I'll assume that U is given in the form of a basis of m linearly independent rational vectors, put as columns into a matrix I am afraid I shall call U from now on. The proof will explain how to find a \mathbb{Z} -basis of the intersection as well as a complement in \mathbb{Z}^n .

For $m \leq n$ define $I_{n,m}$ to be the $n \times m$ matrix

$$I_{n,m} = \begin{bmatrix} I_m \\ 0 \end{bmatrix}.$$

For $i \leq n$ let $e_{i,n}$ be the n -dimensional vector with the i -th coordinate 1 and all others 0.

[5] Lemma. (Explicit saturation) *Suppose U to be an $n \times m$ matrix whose columns are linearly independent rational vectors in \mathbb{Q}^n . We can find a matrix A in $\text{GL}_n(\mathbb{Z})$ and a matrix B in $\text{GL}_m(\mathbb{Q})$ such that AUB is $I_{n,m}$.*

Under the hypothesis of independence, of course $m \leq n$. I recall that $\text{GL}_n(\mathbb{Z})$ is the group of integral matrices of determinant ± 1 , which is to say those integral matrices with integral inverses.

Why does this imply the Lemma? The matrix UB is a new rational basis of the vector space spanned by the columns of U . Since $UB = A^{-1}I_{n,m}$, it is also the first m columns of the matrix A^{-1} , whose columns make up a basis of \mathbb{Z}^n . This is exactly what we want.

Proof. I shall tell exactly how to get A and B . The proof proceeds by induction on m , and the case $m = 1$ is a simple variant of the previous Lemma.

The case $m = 1$ of this asserts that if u is any vector in \mathbb{Q}^n , there exists some b in \mathbb{Q}^\times and an A in $\text{GL}_n(\mathbb{Z})$ such that Aub is the column vector v with $v_1 = 1$, $v_i = 0$ for $i > 1$. We start by multiplying u by some integer p to make pu itself integral. The Lemma in slight disguise now finds A such that $v = Apu$ has all $v_i = 0$ for all $i > 1$, and $v_1 = q$ where q is the gcd of the coefficients pu_i . That is to say, $v = qe_{1,n}$. But then $(p/q)u$ is still integral, and $A(p/q)u = e_{1,n}$.

Now suppose $m > 1$, and assume the Lemma to be true for $m - 1$. We can find A_* and B_* such that A_*uB_* is a matrix whose first $m - 1$ columns are $I_{m-1,n}$:

$$A_*uB_* = \begin{bmatrix} I_{m-1} & u_{m-1} \\ 0 & u_{n-m+1} \end{bmatrix}.$$

Here u_{m-1} is a column vector of length $m - 1$, and u_{n-m+1} one of length $n - m + 1$. Elementary column operations, amounting to multiplication of this on the right by certain triangular matrices, will make $u_{m-1} = 0$, and then we can apply the case $m = 1$ to get $u_{n-m+1} = e_{m,n}$. ◻

The proof tells you how to calculate A and B as you go along, but it also tells you how to calculate A^{-1} and B^{-1} , since, for example, multiplying A on the left by an embedded 2×2 matrix S is no easier than multiplying A^{-1} on the right by S^{-1} , which is trivial to compute.

I'll say that an integral matrix E is in **Hermite normal form** if it looks like

$$\begin{bmatrix} & & & & \\ & & & & \\ & & & & \\ & & & & \\ 0 & H & & & \end{bmatrix},$$

where H is a matrix satisfying certain echelon conditions. Suppose it has d columns. The in each of the last columns j there exists a last non-zero entry, say in row $r(j)$. (a) The entry $p(j) = h_{r(j),j}$ is positive. (b) If $j < k$ then $r(j) < r(k)$. (c) If $k > j$ then $h_{r(j),k}$ is in the range $[0, p(j))$. The general shape of a matrix in Hermite normal form is thus something like

$$\begin{bmatrix} 0 & 0 & * & * & * \\ 0 & 0 & \bullet & * & * \\ 0 & 0 & 0 & * & * \\ 0 & 0 & 0 & \bullet & * \\ 0 & 0 & 0 & 0 & \bullet \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

where $\bullet \neq 0$ and $*$ is arbitrary.

[6] Lemma. (Hermite normal form) *If M is any integral $r \times c$ matrix, one can find B in $\text{GL}_c(\mathbb{Z})$ such that $MB = H$ is in Hermite normal form.*

The non-zero columns of H make up a distinguished basis of the lattice spanned by the columns of M , relative to the standard flag

$$0 \subset \mathbb{Q} \subset \mathbb{Q}^2 \subset \dots \subset \mathbb{Q}^n.$$

Proof. Finding the Hermite normal form of a matrix requires first of all several applications, row by row from the bottom up, of the Euclidean algorithm. This gives conditions (a) and (b). Condition (c) can then be satisfied by applying some elementary column operations. qed

A matrix is said to be in **Smith normal form** (presumably named after the prominent nineteenth century English mathematician Harry Smith) if it looks like

$$\begin{bmatrix} 0 & D \\ 0 & 0 \end{bmatrix},$$

where D is a diagonal matrix with positive entries such that $d_{i,i} | d_{i+1,i+1}$.

[7] Lemma. (Smith normal form) *If M is an integral matrix of size $r \times c$, we can find A in $\text{GL}_r(\mathbb{Z})$ and B in $\text{GL}_c(\mathbb{Z})$ such that $AMB = S$ is in Smith normal form.*

Here, MB is a basis of the lattice L_M generated by the columns of M . If S has k non-zero columns, then since $MB = A^{-1}S$, the first k columns a_i of A^{-1} are part of a basis of \mathbb{Z}^n such that $d_{i,i}a_i$ make up a basis of L_M . The matrix B^{-1} expresses the columns of M in terms of that basis. As earlier, it will be no more difficult to find A^{-1} and B^{-1} than A and B .

Thus finding the Smith normal form is the same as implementing the principal divisor theorem.

Proof. First put the matrix in Hermite normal form. Then multiply it on the left by a matrix in $\text{GL}_r(\mathbb{Z})$ to get it in the form

$$\begin{bmatrix} 0 & d & * & \dots & * \\ 0 & 0 & * & \dots & * \\ \dots & & & & \\ 0 & 0 & * & \dots & * \end{bmatrix}.$$

There are now two possibilities: (i) The corner entry d is the gcd of the first row. We can tell whether this is true by running along the first row, applying an elementary column operation to replace an entry by its remainder upon division by d . If these remainders were all 0, our matrix looks like

$$\begin{bmatrix} 0 & d_{1,1} & 0 & \dots & 0 \\ 0 & 0 & * & \dots & * \\ \dots & & & & \\ 0 & 0 & * & \dots & * \end{bmatrix}.$$

We move on to the next column to get $d_{2,2}$. Etc. (ii) The entry d is not the gcd of the top row, and some of those remainders were not zero. In this case, we apply the Euclidean algorithm to replace d by the gcd of the row. This may, however, place some non-zero integers in the first column, so we have to go back to the start. We keep on applying the Euclidean algorithm to the first column and row, but in each cycle the corner entry decreases, so we must eventually break the loop.

At the end of this part of the computation, we'll have a diagonal matrix D , but one which might not satisfy the divisibility condition. To obtain that, we perform several times an operation essentially in $\text{GL}_2(\mathbb{Z})$. This operation is in effect a special case of our problem. Suppose we are given a diagonal integral matrix

$$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}.$$

We want to multiply on left and right by matrices in $GL_2(\mathbb{Z})$ to get a similar diagonal matrix, but with $a|b$. Let d be the gcd of a and b . Perform the usual Euclidean algorithm to find k and ℓ such that $ka + \ell b = d$. Adding k times the first column to the second gives

$$\begin{bmatrix} a & ka \\ 0 & b \end{bmatrix},$$

and then adding ℓ times the second row to the first gives

$$\begin{bmatrix} a & ka + \ell b \\ 0 & b \end{bmatrix} = \begin{bmatrix} a & d \\ 0 & b \end{bmatrix}.$$

A signed swap of columns gives

$$\begin{bmatrix} d & -a \\ b & 0 \end{bmatrix}.$$

Since d divides both a and b we can subtract b/d times the first row from the second to get

$$\begin{bmatrix} d & -a \\ 0 & ab/d \end{bmatrix};$$

and finally add a/d times the first column to the second to get

$$\begin{bmatrix} d & 0 \\ 0 & ab/d \end{bmatrix}.$$

We apply this operation to a large diagonal matrix several times, to all pairs $d_{i,i}$ and $d_{j,j}$ with $i < j$. First we get $d_{1,1}$ to divide all $d_{j,j}$ with $j > 1$, then get $d_{2,2}$ to divide all $d_{j,j}$ with $j > 2$, etc. qed

Chapter 3 of [Pohst-Zassenhaus:1989] explains in more detail how to compute Hermite and Smith normal forms of an arbitrary integral matrix. In particular, they point out the difficulties that arise, which do not appear in my account. Neither of the two normal forms is usually an easy computation, but finding the Hermite form is noticeably simpler, and it is in any event a good first step towards the Smith form. Among other things it tells us immediately the column rank at hand. In one situation we'll be dealing with, our matrix will start off in a particularly good Hermite form.

[8] Lemma. *The canonical projection from $SL_n(\mathbb{Z})$ to $GL_n(\mathbb{Z}/2) = SL_n(\mathbb{Z}/2)$ is surjective.*

This is a very simple case of the strong approximation theorem for simply connected semi-simple algebraic groups defined over Dedekind domains. In the particular case at hand it is extremely easy to prove and to implement constructively.

Proof. If F is any field, then applying Gauss-Jordan elimination, we may write any matrix in $GL_n(F)$ as $n_1 w a n_2$ where the n_i are upper triangular, a is diagonal, and w is a permutation matrix. We may multiply w by a diagonal matrix with entries ± 1 if necessary to make it a monomial matrix with entries ± 1 and $\det(w) = 1$. The matrices n_i are certainly in the image of the projection, as is w . And in our case, since all units in $\mathbb{Z}/2$ are 1, a happens to be I . qed

The proof of the general result is not so different. Suppose we are given M is $SL_n(\mathbb{Z}/N)$. Factoring N , according to the Chinese Remainder Theorem reduces the problem to the case when N is a prime power p^n . The proof now proceeds by induction on n . It is a very general fact that no matter what the field F the group $SL_n(F)$ (or for that matter any simply connected, semi-simple, split group over F) is generated by upper and lower triangular unipotent matrices, and the case $n = 1$ follows from that (although carrying this out does not lead to the most efficient computation). The case of $n > 1$ is trivial.

4. Proof of the Theorem. We may assume that $L = \mathbb{Z}^n$, and that we are given an integral matrix τ of order 2.

Let M_{\pm} be the intersection of the ± 1 eigenspaces with L . According to the Subspace Saturation Lemma, each of these is a summand of L . Let $M = M_+ \oplus M_-$. If $M = L$, there is no problem—we set $L_{\pm} = M_{\pm}$, $L_{\text{sw}} = \{0\}$. Otherwise, things are more interesting.

An important part of the proof, which in fact motivates it, is to understand how τ acts on the quotient $L/2L$. This is a finite-dimensional vector space over \mathbb{F}_2 . According to the Jordan decomposition theorem it must break up into a direct sum of spaces on which τ acts by

$$\begin{bmatrix} \lambda & 1 & 0 & \dots & 0 \\ 0 & \lambda & 1 & \dots & 0 \\ 0 & 0 & \lambda & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \lambda \end{bmatrix}$$

but since $\tau^2 = 1$ it must in fact be a sum of one-dimensional spaces on which τ is the identity, plus a direct sum of two-dimensional space on each of which τ acts as the matrix

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \quad (\text{over } \mathbb{F}_2).$$

This matrix is equivalent to a swap (in characteristic 2), as we can deduce from the following observation:

[9] Lemma. (Swap Lemma) *The integral matrix*

$$\begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}.$$

is that of a swap.

Proof. If

$$\begin{aligned} \tau(e) &= e \\ \tau(f) &= -f + e \end{aligned}$$

then

$$\tau(e - f) = e - (-f + e) = f$$

so τ swaps $e - f$ and f . □

The lattice decomposition we are looking for is closely related to this decomposition of $L/2L$, except that the two lattices L_{\pm} must both collapse to the single eigenspace modulo 2.

Keeping an example in mind will help make the proof of the Theorem clear. Let $L = \mathbb{Z}^4$, with $\tau e_1 = -e_1$, $\tau e_2 = e_3$, $\tau e_3 = e_2$, $\tau e_4 = e_4$. Here

$$\begin{aligned} M_- &= \mathbb{Z}e_1 \oplus \mathbb{Z}(e_2 - e_3) \\ M_+ &= \mathbb{Z}e_4 \oplus \mathbb{Z}(e_2 + e_3) \end{aligned}$$

and $L/M \cong \mathbb{F}_2$. It is generated by the image of either e_2 or e_3 . This example serves to illustrate that the decomposition is not canonical—for example, the swap component could equally well be spanned by $e_2 + e_1$ and $e_3 + e_1$. I am not aware that this failure plays an important role.

I now start the proof in detail. The first step is to find the Smith normal form of $\tau + I$. This gives us a basis $e_1, \dots, e_j, e_{j+1}, \dots, e_k, e_{k+1}, \dots, e_n$ of L where the $2e_i$ for $i \leq j$ and the e_i for $j < i \leq k$ make up a basis of $(\tau + I)L$. This implies also that the e_i with $i \leq k$ make up a basis of M_+ . The calculation also gives us equations

$$(\tau + I)e_{\ell} = \sum_{i \leq j} 2c_i e_i + \sum_{j < i \leq k} c_i e_i$$

for $\ell > k$. But then

$$(\tau + I)\left(e_\ell - \sum_{i \leq j} c_i e_i\right) = \sum_{i \leq j} 2c_i e_i + \sum_{j < i \leq k} c_i e_i - \sum_{i \leq j} 2c_i e_i = \sum_{j < i \leq k} c_i e_i.$$

If we replace the e_ℓ for $\ell > k$ by $e_\ell - \sum_{i \leq j} c_i e_i$, we see that the lattice L_* spanned by the e_i with $i > j$ is stable under τ , as is its complement, the lattice L_+ spanned by the e_i with $i \leq j$. We can therefore split off L_+ , on which $\tau = I$, and work only with L_* . We may as well take L to be L_* . We may also assume we have a basis e_1, e_2, \dots, e_m of L with the e_i for $i \leq k$ a basis of $(\tau + I)L$ which is now the same as M_+ . With the new basis the matrix of τ is of the form

$$\begin{bmatrix} I & C \\ 0 & -I \end{bmatrix}.$$

Our goal now is to show that L may be decomposed into $L_- \oplus L_{\text{sw}}$.

We next find the Smith normal form of

$$\tau - I = \begin{bmatrix} 0 & C \\ 0 & -2I \end{bmatrix}$$

which means, in effect, finding that of

$$\begin{bmatrix} C \\ -2I \end{bmatrix}.$$

This is already in a particularly good Hermite normal form. Since the pivot entries are all 2, the calculation of its Smith normal form is relatively simple. At any rate, we get a basis f_i of L such that the f_i for $1 \leq i \leq j$ and $2f_i$ for $j < i \leq m - k$ are a basis of $(\tau - I)L$. Let L_- be the lattice spanned by the f_i with $i > j$. As before, we can find a τ -stable complement L_* of L_- , and split off L_- .

As a result of what we have done so far, we have a decomposition $\mathbb{Z}^n = L_+ \oplus L_* \oplus L_-$, where $\tau = \pm I$ on L_\pm . Furthermore, in L_* , which I may as well now take to be L , the intersection M_\pm of the ± 1 -eigenspace of τ coincides with $(\tau \pm I)L$. We also have (a) a basis (e_i) of L such that the e_i with $i \leq k$ form a basis of M_+ and (b) a basis (f_i) ($i \leq m - k$) of M_- , expressed in terms of the e_i .

[10] Lemma. *Suppose τ to be an involution of the lattice L , M_\pm the intersection of the ± 1 -eigenspaces of τ with L . If $(\tau \pm I)L = M_\pm$, then τ is a direct sum of swaps.*

This is really the crux of the proof of the Theorem.

Proof. I claim first that

$$\text{the kernel of the map } (\tau \pm I) \text{ from } L \text{ to } M_\pm/2M_\pm \text{ is } M = M_- \oplus M_+.$$

Because if $(\tau + I)e = 2m = (\tau + I)m$ for m in M_+ , then $(\tau + I)(e - m) = 0$ so that $e - m$ lies in M_- and $e = (e - m) + m$ lies in M . Therefore $\tau \pm I$ is an embedding of the \mathbb{F}_2 -vector space L/M into $M_\pm/2M_\pm$.

As a consequence of this, we must have $m - k = k$, $m = 2k$, and $L/M \cong (\mathbb{Z}/2)^k$.

The e_i with $i \leq k$ and the f_i with $i \leq k$ make up a basis of $M_+ \oplus M_-$. We next find the Smith normal form of the matrix whose columns are these e_i and the f_i , assuming the e_i to be the basis of L . This matrix looks like

$$\begin{bmatrix} I & F_1 \\ 0 & F_2 \end{bmatrix}.$$

Applying elementary column operations, we may reduce this to

$$\begin{bmatrix} I & 0 \\ 0 & G \end{bmatrix}.$$

But since the index of $L/M \cong (\mathbb{Z}/2)^k$, the Smith normal form of G is the diagonal matrix with all diagonal entries equal to 2. Therefore G is itself divisible by 2. So the columns g_i of $G/2$, together with the e_i for $i \leq k$, are a basis of L such that these e_i together with the $2g_i$ are a basis of M .

Now $(\tau + I)$ induces an isomorphism of L/M with $M_+/2M_+ \subseteq L/2L$. The images \bar{g}_i in L/M make up a basis of that vector space over \mathbb{F}_2 , as are the images \bar{e}_i of the e_i in $M_+/2M_+$. We therefore have

$$(\tau + I)\bar{g}_i = \sum \bar{c}_i^j \bar{e}_j$$

where $\bar{C} = (\bar{c}_i^j)$ is an invertible $k \times k$ matrix over \mathbb{F}_2 . Since according to strong approximation the canonical projection from $\mathrm{SL}_n(\mathbb{Z})$ to $\mathrm{SL}_n(\mathbb{Z}/2)$ is surjective, we may replace the basis e_i for M_+ , and assume that $(\tau + I)g_i = e_i$ modulo $2M_+$.

But if $(\tau + I)g_i = e_i + 2m_i$ with m_i in M_+ , then

$$(\tau + I)(g_i - m_i) = e_i + 2m_i - 2m_i = e_i.$$

We may replace the basis g_i by the $g_i - m_i$ so that

$$(\tau + I)g_i = e_i, \quad \tau(g_i) = -g_i + e_i$$

The lattice L is the direct sum of the τ -stable two-dimensional lattices spanned by g_i and e_i , and on this the matrix of τ is

$$\begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}.$$

The Swap Lemma tells us that we are through. qed

This concludes the proof of the Theorem, too. qed

5. The implementation in Atlas. As I have said, the decomposition of a real torus T is not canonical. The good news is that the full decomposition is not necessary for the most important computations in du Cloux's program, which does not use the explicit decomposition but instead just tells you the dimensions of each. What is important is the corollary of the decomposition, the structure of the component group $\pi_0(T(\mathbb{R}))$, or even more significantly its dual. These both have simple characterizations in terms of the involution τ and data which has already been computed in the course of the proof of the Theorem. I'll just look at the dual.

If χ lies in X^T and is fixed by τ , then it takes t in $T(\mathbb{R})$ to \mathbb{R}^\times . If $\chi = \rho^\tau \rho^{-1}$ then for t in $T(\mathbb{R})$

$$\chi(t) = \rho(t)^2$$

and must therefore lie in the connected component $\mathbb{R}^{\mathrm{pos}}$ of \mathbb{R}^\times . We therefore have a canonical map from

$$\frac{\mathrm{Ker}(\tau - I)}{\mathrm{Im}(\tau + I)}$$

to the group of homomorphisms from $T(\mathbb{R})$ to $\mathbb{R}^\times / \mathbb{R}^{\mathrm{pos}} = \{\pm 1\}$, which is the same as the character group of $T(\mathbb{R})$ modulo its connected component. The Theorem immediately implies:

[11] Proposition. *This canonical map is an isomorphism.*

In the proof of the Theorem, one of the first things we did was to compute this group by an application of Smith normal form.

Actually, this Proposition may be proved directly, with no use of the Theorem! If we let $L^\vee = X_*(T)$ and tensor with the exact sequence induced by the exponential map $z \mapsto e^{2\pi iz}$

$$0 \rightarrow \mathbb{Z} \rightarrow \mathbb{C} \rightarrow \mathbb{C}^\times \rightarrow 1$$

with L^\vee we get

$$0 \rightarrow L^\vee \rightarrow L^\vee \otimes \mathbb{C} \rightarrow T(\mathbb{C}) \rightarrow 1.$$

Let Gal be the Galois group of \mathbb{C}/\mathbb{R} . If A is the maximal split real torus in T the associated long exact cohomology sequence gives us

$$0 \rightarrow (L^\vee)^{\text{Gal}} = X_*(A) \rightarrow (L^\vee \otimes \mathbb{C})^{\text{Gal}} \rightarrow T(\mathbb{R} \rightarrow H^1(\text{Gal}, L^\vee)) \rightarrow 0.$$

which identifies $T(\mathbb{R})$ modulo its connected component with $H^1(\text{Gal}, L^\vee)$, the dual of $\text{Ker}(\tau - I)/\text{Im}(\tau + I)$. This observation was made by Robert Kottwitz, and indeed a much more general result valid for all local fields can be found in §3.3 of his 1984 paper.

One consequence of the Theorem is that although the split factor of a real torus is not canonical, its dimension is that of the \mathbb{F}_2 -vector space

$$\frac{\text{Ker}(\tau - I)}{\text{Im}(\tau + I)}.$$

Similarly, the dimension of the compact factor is the \mathbb{F}_2 -dimension of

$$\frac{\text{Ker}(\tau + I)}{\text{Im}(\tau - I)}.$$

The dimension of the \mathbb{C}^\times factor is the complement of these. Thus although the factorization is not unique, the dimensions of its factors are. These dimensions are computed by `Atlas`, using the Smith normal form as in the proof of the Theorem given here.

The principal relevant module of `Atlas` is `structure/tori.cpp`. Reading the documentation in the file is instructive, but one should realize that there, as in just about all of the project, `du Cloux` has used the Cartan involution $-\tau$ instead of the Galois involution τ . A principal task of the program is to construct representatives of all the conjugacy classes of real tori in a given reductive group. There are two natural ways to do this, starting with either the maximally compact maximal torus or the maximally split one. `Du Cloux` has chosen the second, and the tori are constructed from that maximally compact torus by applying Cayley transforms. How he does this, and how keeps track of the Cartan involution of the tori, is a story that is partly told in the notes on combinatorics and real groups by `du Cloux` listed among the references.

Incidentally, the documentation in version 3 of `tori.cpp` is significantly better than that in older versions, but as far as I can see the author (who cannot be `du Cloux`) is not named.

6. Langlands' parametrization of characters. One simple case of a relatively deep theorem of Langlands is that if F is either \mathbb{C} or \mathbb{R} , the complex characters

$$T(F) \rightarrow \mathbb{C}^\times$$

possess an extremely important if rather subtle parametrization in terms of **Weil groups** and dual tori.

If F is any local field, either p -adic or real (i. e. \mathbb{R} or \mathbb{C}), and K/F is a Galois extension, say of degree n , the Weil group $W_{K/F}$ fits into an extension

$$1 \rightarrow K^\times \rightarrow W_{K/F} \rightarrow \text{Gal}(K/F) \rightarrow 1.$$

The group $\text{Gal}(K/F)$ here acts by conjugation on K^\times and the extension is highly non-trivial. More precisely, one of the main results of local class field theory is that the cohomology group $H^2(\text{Gal}(K/F), K^\times)$ parametrizing extensions is canonically isomorphic to \mathbb{Z}/n , and the one defining the Weil group has invariant $1/n$.

If $F = \mathbb{C}$ then there are no algebraic extension fields, and $W_{\mathbb{C}} = W_{\mathbb{C}/\mathbb{C}} = \mathbb{C}^\times$. If $F = \mathbb{R}$, the only extension is \mathbb{C} . The group $W_{\mathbb{C}/\mathbb{R}}$ is generated by \mathbb{C}^\times and an element σ such that $\sigma^2 = -1$ and $\sigma z = \bar{z}\sigma$ for z in \mathbb{C}^\times . We have an exact sequence

$$1 \rightarrow \mathbb{C}^\times \rightarrow W_{\mathbb{R}} \rightarrow \mathcal{G} = \text{Gal}(\mathbb{C}/\mathbb{R}) \rightarrow 1$$

in which σ maps onto conjugation. It is not an accident that this group embeds into the quaternion algebra—it is a basic fact that local Weil groups always embed into local division algebras. If F is p -adic, the Weil group $W_{K/F}$

is very closely related to the Galois group of the maximal abelian extension of K as an extension of F , but for \mathbb{R} and \mathbb{C} their true significance is somewhat hidden from us.

It is a fundamental theorem of local class field theory that in all cases there exists a norm map from $W_{K/F}$ to F^\times that agrees with the norm $N_{K/F}$ on K^\times and identifies F^\times with the maximal abelian quotient of $W_{K/F}$. In the case of \mathbb{C}/\mathbb{R} the norm map takes z to $z\bar{z}$ and σ to -1 , and the assertion may be verified directly—we have

$$\sigma z \sigma^{-1} z^{-1} = \bar{z}/z$$

and the map taking z to \bar{z}/z wraps \mathbb{C}^\times around the unit circle, the kernel of $N_{\mathbb{C}/\mathbb{R}}$.

The Weil group is one ingredient in Langlands' parametrization. The other is the **Langlands dual torus** ${}^L T$ associated to any algebraic torus defined over a local field. Here, suppose T to be an algebraic torus defined over \mathbb{C} or \mathbb{R} . Let's look first at \mathbb{C} . The group $T(\mathbb{C})$ may be identified with $\text{Hom}(X^*(T), \mathbb{C}^\times)$. The **dual** complex torus \widehat{T} is $\text{Hom}(X_*(T), \mathbb{C}^\times)$. This is also the full Langlands dual group ${}^L T$.

If T is defined over \mathbb{R} , the Galois group \mathcal{G} acts on $\widehat{T}(\mathbb{C})$ through its action on $X^*(T)$, and the Langlands dual group ${}^L T$ is defined to be the semi-direct product of \widehat{T} by \mathcal{G} .

Why are the Weil groups and Langlands duals important for algebraic tori defined over local fields? Suppose F to be any local field and T an algebraic torus defined over F . Suppose in addition that K/F is a Galois extension such that over K T becomes isomorphic to a product of copies of \mathbb{G}_m . Langlands' theorem is that the complex characters of $T(F)$ are parametrized naturally by continuous splittings of the extension

$$1 \rightarrow \widehat{T}(\mathbb{C}) \rightarrow {}^L T \rightarrow W_{K/F} \rightarrow 1$$

modulo conjugation by $\widehat{T}(\mathbb{C})$ —in other words, by $H^1(W_{K/F}, \widehat{T}(\mathbb{C}))$. For \mathfrak{p} -adic fields, the proof requires all of the machinery of local class field theory. But for $F = \mathbb{C}$ it is just about trivial, and for $F = \mathbb{R}$ it follows easily from the classification of real tori. In fact, the proof of the claim for these cases given by Langlands in [Langlands:1974] is very close to a proof of the classification Theorem.

In order to prove the assertion, it suffices to prove it for the single complex torus and also for each of the three irreducible real tori.

- Suppose $k = \mathbb{C}$. Then $W_k = \mathbb{C}^\times$, and all tori are products of \mathbb{C}^\times . We thus want to verify that $\text{Hom}(T, \mathbb{C}^\times)$ with $\text{Hom}(\mathbb{C}^\times, \widehat{T})$ (where Hom for the moment means continuous homomorphisms). But if L^\vee is the cocharacter lattice of T then $\widehat{T} = \text{Hom}(L^\vee, \mathbb{C}^\times)$, so for elementary reasons

$$\begin{aligned} \text{Hom}(\mathbb{C}^\times, \widehat{T}) &= \text{Hom}(\mathbb{C}^\times, \text{Hom}(L^\vee, \mathbb{C}^\times)) \\ &= \text{Hom}(L^\vee \otimes \mathbb{C}^\times, \mathbb{C}^\times) \\ &= \text{Hom}(T(\mathbb{C}), \mathbb{C}^\times). \end{aligned}$$

In practice, it is useful to have at hand an explicit description of the characters of a complex torus. The characters of \mathbb{C}^\times can be described as $z \mapsto |z|^s z^n$ for some s in \mathbb{C} , n in \mathbb{Z} . In a symmetric version, this is to be seen as $z \mapsto z^a \bar{z}^b$ for various complex numbers a, b with $a - b$ in \mathbb{Z} . Of course neither factor is unambiguous, so we need to specify how this is to be interpreted. If $a = b + n$ then we set

$$z^a \bar{z}^b = z^{b+n} \bar{z}^b = |z|^{2b} z^n.$$

The analogous description of the continuous characters of any complex torus T is through a pair λ, μ in $X^*(T) \otimes \mathbb{C}$ with $\lambda - \mu \in X^*(T)$:

$$\chi_{\lambda, \mu}(\alpha^\vee(z)) = z^{\langle \lambda, \alpha \rangle} \bar{z}^{\langle \mu, \alpha \rangle}$$

for any α in $X_*(T)$. This makes sense since by assumption $\langle \lambda - \mu, \alpha \rangle \in \mathbb{Z}$.

- Suppose $k = \mathbb{R}$. It suffices to verify Langlands' duality for each of the three irreducible real tori.

If $T(\mathbb{R}) = \mathbb{R}^\times$, the assertion is immediate from the identification of the maximal abelian quotient of $W_{\mathbb{R}}$ with \mathbb{R}^\times .

If T is the real torus whose group of points is \mathbb{C}^\times , then it is also the real torus obtained from the trivial one-dimensional torus over \mathbb{C} by what is called **restriction of scalars** from \mathbb{C} to \mathbb{R} . The group \widehat{T} is the group induced by \mathbb{C}^\times from $W_{\mathbb{C}}$ to $W_{\mathbb{R}}$. We have an isomorphism

$$H^1(W_{\mathbb{R}}, \widehat{T}) = H^1(W_{\mathbb{C}}, \mathbb{C}^\times)$$

by Shapiro's Lemma, which implies that Langlands' duality for T in this case is equivalent to it for the original complex group. In explicit terms, the character of \mathbb{C}^\times parametrized by a, b corresponds to the homomorphism from $W_{\mathbb{R}}$ to \widehat{T} taking

$$z \mapsto (z^a \bar{z}^b, z^b \bar{z}^a), \quad \sigma \mapsto ((-1)^{a-b}, 1).$$

The second map may be replaced by

$$\sigma \mapsto ((-1)^{a-b} s, s^{-1}).$$

All choices of $s \neq 0$ are conjugate in ${}^L T T$.

Suppose $T(\mathbb{R}) = \mathbb{S}$. This embeds into \mathbb{C}^\times , and its group of characters is a quotient of the character group of \mathbb{C}^\times . Explicitly, the character of \mathbb{C}^\times parametrized by (a, b) restricts to the character of \mathbb{S} taking z to z^{a-b} .

On the other hand the L -group of \mathbb{C}^\times projects to that for \mathbb{S} :

$$(x, y) \mapsto xy^{-1}$$

is the map on connected components. It is an easy exercise to see that the identification of $H^1(W_{\mathbb{R}}, \widehat{\mathbb{S}})$ with the character group of \mathbb{S} we get through the analogous identification for \mathbb{C}^\times is valid. In other words, on the one hand the characters of \mathbb{S} are all of the form $z \mapsto z^n$. On the other, for each n we can define a map from $W_{\mathbb{R}}$ to ${}^L T$ by mapping z to (z^n, \bar{z}^n) and then to $(z/\bar{z})^n, \sigma$ to $(1, \sigma)$. These correspond.

These assignments might seem a bit arbitrary. Telling whether they are correct or not, as suggested by our remarks in the introduction, is ultimately a global matter—*does this assignment for real places fit in with the parametrization for other places to give rise to L -functions with the right functional equations?* This is shown (albeit only implicitly) by Langlands in his note on automorphic forms on tori, and sketched by Borel in §8 of his Corvallis talk. However, it is easy to check that the parametrization of the characters of \mathbb{C}^\times and \mathbb{R}^\times is correct since they occur in abelian L -functions, and it is also easy to check that it is compatible with the inclusion of \mathbb{S} in \mathbb{C}^\times .

7. References.

- Fokko du Cloux, 'Combinatorics for the representation theory of real groups', available at <http://www.liegroups.org/papers/summer05/combinatorics.pdf>
- ——— *et al.*, documentation for the source code of Atlas at <http://www.liegroups.org/software/>

and in particular the file `tori.cpp` in the package.

- R. E. Kottwitz, 'Stable trace formula: cuspidal tempered terms', *Duke Mathematics Journal* **51** (1984), 611–650.
- R. P. Langlands, 'On the classification of irreducible representations of real algebraic groups', I. A. S. preprint, 1974. Published later as pages 101–170 in **Representation Theory and Harmonic Analysis on Semisimple Lie Groups**, edited by P. Sally and D. Vogan, American Mathematical Society, 1989.
- M. Pohst and H. Zassenhaus, **Algorithmic algebraic number theory**, Cambridge University Press, 1989.