Groups, Matrices and Lattices in Smith Normal Form.

The following is done in three dimensions, for convenience, but it applies in any dimension.

Groups. Begin with the simplest case. Let N be an integer non-singular matrix. Its columns represent the basis for a subgroup $\mathcal{L}_N$ (superlattice) of $\mathbb{Z}^3$.

Since $\mathbb{Z}^3$ and its subgroups are Abelian, we know that all the subgroups are *normal* so there exists a quotient group $G = \mathbb{Z}^3/\mathcal{L}_N$, and that group is *finite*. In fact, each coset has exactly one representative in each tile, so the order of G is equal to the absolute value of the determinant of N. Since G is also Abelian, it must be a direct sum of cyclic groups – by the Fundamental Theorem of Finite Abelian Groups.

Recall that one canonical form for such direct sums is called Smith Normal Form, where the direct summands are arranged in such a way that the order of each summand must divide the next. In other words, $G = \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_k}$ where $m_1|m_2|\ldots m_{k-1}|m_k$ and (of course) $\prod m_i = |G|$. Any finite Abelian group can be written in this form, and the expression is unique. (Isomorphic groups will yield the same "invariant factors" when written in this form.)

Note that, since $G = \mathbb{Z}^3/\mathcal{L}_N$, there must be a homomorphism ψ from $\mathbb{Z}^3$ onto G, having $\mathcal{L}_N$ as its kernel. In other words, $\mathcal{L}_N = \{p \in \mathbb{Z}^3 \,:\, \psi(p) = 0\}$. Our task is to find that useful homomorphism.

Matrices. There is also an algorithm for reducing integer matrices to something called Smith Normal Form (or SNF). By elementary integer row and column operations, one can effectively wrangle the gcd of all entries of N into the upper left corner, and then use that element to zero out the remaining elements in first row and first column. We may then do the same thing to the smaller matrix where the first row and column are ignored, etc. Eventually, we obtain an integer diagonal matrix D with each diagonal entry dividing the next one down (just like the SNF for Abelian groups.) Of course its determinant is the same in absolute value as the matrix N that we started with.

Not surprisingly, there's a connection between SNF for Abelian groups and SNF for integer matrices. As you might guess, the SNF form of the basis matrix N effectively tells us how to represent the quotient group $\mathbb{Z}^3/\mathcal{L}_N$ as a direct sum of cyclic groups, and it will also give us the homomorphism ψ suggested above, as well.

The connection. In the matrix case, since the operations are elementary row and column operationss, we have $D = LNR$ where L and R are integer matrices with determinant ± 1 representing the accumulated row operations and column operations respectively. Note that, since R represents elementary column operations, the product NR simply represents a change of basis from N to a new basis $N' = NR$. In other words, the columns of NR are still a basis for $\mathcal{L}_N$. But the new basis has the property that $LN' = D$. That means that every element $w = N'z$ of $\mathcal{L}_N$ (where z is any column of integers) will satisfy the equation $Lw = Dz$.

In other words, if w is any element of our superlattice (subgroup), then Lw will be a vector whose entries are *multiples* of the corresponding diagonal entries in D. To put it another way, if $x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$, let $x^* = (x_1 \pmod{\mathrm{D}_{11}}, x_2 \pmod{\mathrm{D}_{22}}, x_3 \pmod{\mathrm{D}_{33}})$. Then we have shown $w \in \mathcal{L}_N$ iff $(Lw)^* = (0,0,0)$ (the zero-element in the group $G_0 = \mathbb{Z}_{D_{11}} \oplus \mathbb{Z}_{D_{22}} \oplus \mathbb{Z}_{D_{33}}$.

That suggests we let $\psi(w) = (Lw)^*$, a homomorphism from $\mathbb{Z}$ onto the direct-sum G_0. Then, since that homomorphism is easily shown to be onto, and its kernel is $\mathcal{L}_N$, we see – by the First Isomorphism Theorem of group theory – that $G_0 \cong \mathbb{Z}^3/\mathcal{L}_N$, and ψ is precisely the homomorphism we sought.

Thus we have connected the two versions of SNF. The matrix algorithm, by the diagonal entries in D, provides the SNF description of the quotient group, and the transition matrix L provides the homomorphism which projects the parent lattice onto the group.

An example. Let $N = \begin{pmatrix} 1 & 2 & -1 \\ 1 & 4 & -3 \\ 0 & 2 & 4 \end{pmatrix}$. This describes a lattice $\mathcal{L}_N$ which contains the points $p_1 = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$, $p_2 = \begin{pmatrix} 2 \\ 4 \\ 2 \end{pmatrix}$, and $p_3 = \begin{pmatrix} -1 \\ -3 \\ 4 \end{pmatrix}$, and *all* the points which are integer linear combinations of those three points. The matrix N has determinant 12, which must be the volume of each lattice tile – and it is also the order of the quotient group $\mathbb{Z}^3/\mathcal{L}_N$.

Using the SNF algorithm to diagonalize this basis matrix, we find $D = LNR$ where $D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 6 \end{pmatrix}$, with $L = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & -1 & -2 \end{pmatrix}$ and $R = \begin{pmatrix} 1 & 7 & 11 \\ 0 & -1 & -2 \\ 0 & 1 & 1 \end{pmatrix}$. [Note that someone else might obtain a different L and R, but the *same* D.]

Thus we now know that the quotient group is $G = \mathbb{Z}^3/\mathcal{L}_N \cong \mathbb{Z}_1 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6$ (since the group $\mathbb{Z}_1$ is just the identity).

Further, from the matrix L, we may obtain the homomorphism projecting $\mathbb{Z}^3$ onto the quotient group, with kernel $\mathcal{L}_N$. If $w = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$ then $\psi(w) = (Lw)^* = \begin{pmatrix} y \pmod 1 \\ z \pmod 2 \\ x - y - 2z \pmod 6 \end{pmatrix}$. Thus the point (x, y, z) in the integer lattice $\mathbb{Z}^3$ projects to the point $\big(z \pmod 2,\ x - y - 2z \pmod 6\big) = \big(z \pmod 2,\ x + 5y + 4z \pmod 6\big)$ in the quotient group $\mathbb{Z}_2 \oplus \mathbb{Z}_6$ (noting that anything mod 1 is zero).

Note that this homomorphism also provides a different, but convenient way to describe the subgroup lattice. Since $\mathcal{L}_N$ is the kernel of ψ, it is comprised of the points $(x, y, z) \in \mathbb{Z}^3$ which satisfy the simultaneous congruences $z \equiv 0 \pmod 2$ and $x + 5y + 4z \equiv 0 \pmod 6$. We note that all three basis points p_1, p_2 and p_3 satisfy these congruences, and thus so will all their integer linear combinations (all points in $\mathcal{L}_N$).

Rows versus columns – left versus right. Note that, in this presentation, where we regarded N as a *column* basis, the matrix R turned out to be merely a basis change, while L turned out to represent the homomorphism from the parent lattice onto the finite group with moduli from the diagonal elements of D. *But if we had taken N to be a row-basis instead of column basis, the roles of L and R would be reversed. L would then represent the change to a more convenient basis, and the columns of R would represent the homomorphism onto the finite group.*

In either case, note that L and R and the homomorphism ψ are *not unique*. A different application of SNF to N might have yielded different L and R, but the same D. We'd then have an equivalent homomorphism from $\mathbb{Z}^3$ onto the *same* group G, with the same kernel.

In the example we computed above, for instance, a different application of the SNF matrix algorithm, with the same N, might have yielded the same diagonal $D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 6 \end{pmatrix}$, but different $L = \begin{pmatrix} 1 & 0 & 0 \\ -5 & 3 & 1 \\ -2 & 2 & 1 \end{pmatrix}$ and $R = \begin{pmatrix} 0 & -1 & 2 \\ 0 & 0 & 1 \\ -1 & -1 & 4 \end{pmatrix}$, which would change the homomorphism to $(x, y, z) \mapsto \big(-5x + 3y + z \pmod 2,\ -2x + 2y + z \pmod 6\big) = \big(x + y + z \pmod 2,\ 4x + 2y + z \pmod 6\big)$.

The new homomorphism is distinctly different, since $(1, 0, 1) \mapsto (0, 5)$ now, where previously $(1, 0, 1)$ was mapped to $(1, 5)$ in the group. But the *kernel* is the same. Note that the new simultaneous congruences $x + y + z \equiv 0 \pmod 2$ and $4x + 2y + z \equiv 0 \pmod 6$ are *mathematically equivalent* to the previous pair of congruences we obtained: $z \equiv 0 \pmod 2$ and $x + 5y + 4z \equiv 0 \pmod 6$. They describe the same kernel $\mathcal{L}_N$.

[The reader may find it interesting to note that the relationship between these two homomorphisms, and the corresponding pairs of congruences, is given by a particular automorphism of the group G, namely $(g, h) \mapsto (g, h)\begin{pmatrix} 1 & 3 \\ 1 & 4 \end{pmatrix}$ (note the invertible integer matrix). Thus if $g = z$ and $h = x + 5y + 4z$ (the first homomorphism), then $(g, h)\begin{pmatrix} 1 & 3 \\ 1 & 4 \end{pmatrix} = (x + y + z, 4x + 2y + z) \mod (2, 6)$ (the second homomorphism).] I don't know if this is helpful, or simply confusing.

More general lattices. Now, what about the more complicated situation, where N represents a (possibly HNF) matrix describing the change from some lattice other than $\mathbb{Z}^3$ to one of its subgroups (superlattice)?

Then we have a basis B and lattice $\mathcal{L}_B$ and a new basis $C = BN$ for a new lattice $\mathcal{L}_C$. Again, the quotient group $G = \mathcal{L}_B/\mathcal{L}_C$ is Abelian of order $|\det(N)|$. Again, G is a direct sum of cyclic groups corresponding to the diagonal entries of $D = LNR$ (where D is the SNF of N).

The only difference here is that the homomorphism ψ provided by L must depend on the basis B (which might even be irrational). Every point in $\mathcal{L}_B$ has the form $x = Bw$ where w is a column of integers. Then $\psi(x) = Lw$ (modded by the corresponding entries from $D = LNR$). We could write it as $\psi(x) = \big(LB^{-1}x\big)^*$ (with the entries appropriately modded and transposed to a horizontal vector).

More general example. Suppose $\mathcal{L}_B$ is the lattice defined by (columns of) the basis matrix $B = \begin{pmatrix} 1 & 1/2 & 0 \\ 0 & \sqrt{3}/2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$, and $\mathcal{L}_C$ is the subgroup lattice defined by the basis marix $C = BN$, with $N = \begin{pmatrix} 4 & 2 & 2 \\ 2 & 2 & 2 \\ 4 & 0 & 4 \end{pmatrix}$. In other words, one basis for $\mathcal{L}_C$ is given by the columns of

$$C = \begin{pmatrix} 5 & 3 & 3 \\ \sqrt{3} & \sqrt{3} & \sqrt{3} \\ 8 & 0 & 8 \end{pmatrix}.$$

Applying (via Maple) the SNF algorithm to N yields

$$D = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 0 & -1 \\ 1 & -1 & -1 \\ -6 & 4 & 5 \end{pmatrix} N \begin{pmatrix} -2 & -3 & -2 \\ 2 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

Thus our quotient group is $G = \mathcal{L}_B/\mathcal{L}_C \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4$ and $L = \begin{pmatrix} 1 & 0 & -1 \\ 1 & -1 & -1 \\ -6 & 4 & 5 \end{pmatrix}$ so

$$LB^{-1} = \begin{pmatrix} 1 & -\sqrt{3}/3 & -1/2 \\ 1 & -\sqrt{3} & -1/2 \\ -6 & 14\sqrt{3}/3 & 5/2 \end{pmatrix},$$

which provides our homomorphism $\psi(x) = \left(LB^{-1}x\right)^*$ from $\mathcal{L}_B$ onto G.

If we let $x = \begin{pmatrix} 2 \\ \sqrt{3} \\ 2 \end{pmatrix}$, which is an element of $\mathcal{L}_B$ but not of $\mathcal{L}_C$, then $LB^{-1}x = \begin{pmatrix} 0 \\ -2 \\ 7 \end{pmatrix}$ and $\psi(x) = (0, 0, 3) \in G$ (after modding the elements by 2, 2 and 4 respectively). On the other hand, if we let $x = \begin{pmatrix} 7 \\ \sqrt{3} \\ 8 \end{pmatrix}$, which *is* an element of $\mathcal{L}_C$ (the kernel), then $LB^{-1}x = \begin{pmatrix} 2 \\ 0 \\ -8 \end{pmatrix}$ and $\psi(x) = (0, 0, 0)$.

As expected, the elements of $\mathcal{L}_B$ are all mapped to elements of the direct-sum group G and, in particular, the elements of $\mathcal{L}_C$ get mapped to the zero element of the group. The cosets of this quotient group are the distinct translates of $\mathcal{L}_C$ within $\mathcal{L}_B$, and each such translate is assigned a *different* element of the group G.