Remarks on Semidirect Products

If H and K are groups and $u : H \to \mathrm{Aut}(K)$ is a homomorphism, then there is the associated semidirect product group $G(u)$. As a set, $G(u) = K \times H$. The product is $(k', h')(k, h) = (k'(k^{u(h')}), h'h)$, where $k^{u(h')}$ means the result of applying automorphism $u(h')$ to k. All semidirect products of K by H arise this way. The trivial homomorphism $u(h) = \mathrm{id}$, for all $h \in H$, yields the direct product group $K \times H$. If there are no non-trivial homomorphisms $u : H \to \mathrm{Aut}(K)$, then the direct product is the only semidirect product of K by H.

There is an action of the group $\mathrm{Aut}(H) \times \mathrm{Aut}(K)$ on the set $\mathrm{Hom}(H, \mathrm{Aut}(K))$. If a is an automorphism of H and b is an automorphism of K then $(a, b)u$ is the composition $C(b)ua^{-1} : H \to H \to \mathrm{Aut}(K) \to \mathrm{Aut}(K)$, where $C(b)$ is the inner automorphism of $\mathrm{Aut}(K)$ given by conjugation by b.

If $(a, b)u = v$ then groups $G(u)$ and $G(v)$ are isomorphic. Therefore if any two non-trivial homomorphisms u and v are in the same orbit, then up to isomorphism there is only one non-trivial semidirect product of K by H. This observation leads to the classification of groups of order p^3, p an odd prime. A non-abelian group G of order p^3, p an odd prime, will be a semidirect product of either $K = \mathbb{Z}/(p) \times \mathbb{Z}/(p)$ by $H = \mathbb{Z}/(p)$ or $K = \mathbb{Z}/(p^2)$ by $H = \mathbb{Z}/(p)$, depending on whether G does not or does contain an element of order p^2. In each case, there is only one nontrivial $\mathrm{Aut}(H) \times \mathrm{Aut}(K)$ orbit in $\mathrm{Hom}(H, \mathrm{Aut}(K))$. [See below.]

If there is more than one $\mathrm{Aut}(H) \times \mathrm{Aut}(K)$ orbit in the set $\mathrm{Hom}(H, \mathrm{Aut}(K))$, then one needs additional hypotheses before one can understand the isomorphism classes of semidirect products of K by H. The difficulty is that in general u, v in the same orbit is a sufficient but not necessary condition for $G(u)$ to be isomorphic to $G(v)$. However, if K is abelian and if $\gcd(|H|, |K|) = 1$ then $G(u)$ is isomorphic to $G(v)$ if and only if $v = (a, b)u$ for some $(a, b) \in \mathrm{Aut}(H) \times \mathrm{Aut}(K)$.

In practice, the usefulness of this result towards classifying semidirect products up to isomorphism is limited by the difficulties of determining $\mathrm{Aut}(H)$, $\mathrm{Aut}(K)$, $\mathrm{Hom}(H, \mathrm{Aut}(K))$, and the corresponding orbits if either H or K is very complicated.

Anytime $\mathrm{Aut}(K)$ is abelian then conjugation in $\mathrm{Aut}(K)$ is trivial. Therefore, the $\mathrm{Aut}(H) \times \mathrm{Aut}(K)$ action on $\mathrm{Hom}(H, \mathrm{Aut}(K))$ reduces to simply the $\mathrm{Aut}(H)$ action. The orbit of $u : H \to \mathrm{Aut}(K)$ consists of all compositions $ua : H \to H \to \mathrm{Aut}(K)$, where a is an automorphism of H. Note that u and ua have exactly the same image in $\mathrm{Aut}(K)$. Therefore homomorphisms u, v with different images must lie in different $\mathrm{Aut}(H)$ orbits.

If H is cyclic or a $\mathbb{Z}/(p)$-vector space for some prime p, and if $\mathrm{Aut}(K)$ is abelian then it is a nice exercise to show that two homomorphisms $u, v : H \to \mathrm{Aut}(K)$ are in the same orbit if and only if u and v have the same image, that is $u(H) = v(H) \subset \mathrm{Aut}(K)$.

[In the case $H = \mathbb{Z}/(m)$, this should be the same exercise that for any divisor d of m, the natural projection $\pi : (\mathbb{Z}/(m))^* \to (\mathbb{Z}/(d))^*$ is onto. This is trickier than it might look, since it is not a trivial consequence of the tautology that $\mathbb{Z}/(m) \to \mathbb{Z}/(d)$ is onto. But it is easy enough if you use the Chinese Remainder Theorem. In the case H a $\mathbb{Z}/(p)$-vector space, any image is also a $\mathbb{Z}/(p)$-vector space. The claim is then just simple linear algebra. Two linear *surjections* $V \to W$ of vector spaces over any field are in the same $GL(V)$ orbit.]

Suppose $K = \mathbb{Z}/(n)$ is cyclic. Then $\mathrm{Aut}(K) = (\mathbb{Z}/(n))^*$, which is abelian and 'easily' computed as a finite abelian group, using the Chinese Remainder Theorem and the answers for n a prime power. If K is finite abelian but not cyclic then $\mathrm{Aut}(K)$ is never abelian.

If q is an odd prime, $(\mathbb{Z}/(q^n))^*$ is cyclic. Therefore, if H is a $\mathbb{Z}/(q)$-vector space, there is exactly one non-abelian semidirect product of $\mathbb{Z}/(q^n)$ by H, because there is only one non-trivial $\mathrm{Aut}(H)$ orbit. The same statements are true if $H = \mathbb{Z}/(q^s), s > 1$ and $K = \mathbb{Z}/(q^2)$.

Suppose $H = \mathbb{Z}/(q^s)$, $s > 1$ and $K = \mathbb{Z}/(q^n)$, $n > 2$. Now the $\mathrm{Aut}(\mathbb{Z}/(q^s))$ orbits of $u : \mathbb{Z}/(q^s) \to$

$(\mathbb{Z}/(q^n))^*$ correspond bijectively to the possible image groups of u, which are just characterized by their order. There is more than one orbit, so the present methods don't automatically classify isomorphism classes of semidirect products of $\mathbb{Z}/(q^n)$ by $\mathbb{Z}/(q^s)$, since the orders of H and K are not relatively prime. However, you can show that if the images of two us have different orders then the centers of the two $G(u)$s are not isomorphic. So, the orbit classification gives a good start on the classification in this case, and the classification can be finished up by other methods. As a specific example, there are two distinct non-abelian semidirect products of $\mathbb{Z}/(27)$ by $\mathbb{Z}/(9)$.

If $K = (\mathbb{Z}/(q))^n$ for some prime q, then $\mathrm{Aut}(K) = GL(n, \mathbb{Z}/(q))$, the full linear group. One can calculate the order of this group pretty easily. $|GL(n, \mathbb{Z}/(q))| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})$. [This just counts invertible matrices by looking at the choices for the columns. The first column can be any non-zero vector. Each new column cannot be in the subspace spanned by the preceding columns.] For certain orders $|H|$ relatively prime to q, it may be that the image of any $u : H \to K$ is forced to lie in some p-Sylow subgroup of $GL(n, \mathbb{Z}/(q))$. Finding this, you still need to understand orbits.

All p-Sylow subgroups are conjugate, so, in the situation of the above paragraph, using the $\mathrm{Aut}(K)$ part of $\mathrm{Aut}(H) \times \mathrm{Aut}(K)$, you may as well assume $u, v : H \to GL(n, \mathbb{Z}/(q))$ both have images contained in one fixed p-Sylow subgroup of $GL(n, \mathbb{Z}/(q))$. If this Sylow subgroup is just $\mathbb{Z}/(p)$ and if H is cyclic or a $\mathbb{Z}/(p)$-vector space, there is only one non-trivial $\mathrm{Aut}(H)$ orbit of maps $H \to \mathbb{Z}/(p)$. If the p-Sylow subgroup of $GL(n, \mathbb{Z}/(q))$ is not cyclic, you probably can't go further with this approach. For one thing, you may not even see the structure of the p-Sylow subgroup. For another, you probably haven't really exploited all of the $\mathrm{Aut}(K)$ conjugation, you've only brought one Sylow subgroup to another, and maybe you can move that Sylow subgroup around inside itself with more conjugation. So, the $\mathrm{Aut}(H) \times \mathrm{Aut}(K)$ orbits get pretty obscure.

Note that the q-Sylow subgroup of $GL(2, \mathbb{Z}/(q))$ is just $\mathbb{Z}/(q)$. Therefore if H is $\mathbb{Z}/(q^s)$ or a $\mathbb{Z}/(q)$-vector space, there is exactly one non-abelian semidirect product of $(\mathbb{Z}/(q))^2$ by H, since there is only one nontrivial $\mathrm{Aut}(H) \times \mathrm{Aut}(K)$ orbit in $\mathrm{Hom}(H, \mathrm{Aut}(K))$.

You can also sometimes use linear algebra to study semidirect products when $K = (\mathbb{Z}/(q))^n$ and $H = \mathbb{Z}/(m)$ is cyclic. A homomorphism $u : \mathbb{Z}/(m) \to GL(n, \mathbb{Z}/(q))$ 'is' a matrix T with $T^m - 1 = 0$. By factoring $T^m - 1$, you can identify the possible minimal polynomials of T and its possible invariant factors, hence the possible conjugate classes of such T. Here are a couple examples.

Classify semidirect products of $(\mathbb{Z}/(3))^3$ by $\mathbb{Z}/(4)$. Now $T^4 - 1 = (T - 1)(T + 1)(T^2 + 1)$. The minimal polynomial of a non-trivial $T \in GL(3, \mathbb{Z}/(3))$ must be $(T+1)$, $(T-1)(T+1)$, $(T-1)(T^2+1)$, or $(T + 1)(T^2 + 1)$. This results in $1 + 2 + 1 + 1 = 5$ conjugate classes of such 3×3 matrices over $\mathbb{Z}/(3)$. This doesn't quite mean yet that there are 5 isomorphism classes of non-abelian semidirect products. It could happen that a matrix T and its inverse are not themselves conjugate, but using the $\mathrm{Aut}(H) = \mathrm{Aut}(\mathbb{Z}/(4))$ action we clearly see that T and T^{-1} define isomorphic groups. But in this case, it is easy to see any such T is conjugate to its inverse, hence the $\mathrm{Aut}(K)$ orbits are the same as the $\mathrm{Aut}(H) \times \mathrm{Aut}(K)$ orbits.

Classify semidirect products of $(\mathbb{Z}/(11))^2$ by $\mathbb{Z}/(5)$. Now $T^5 - 1 = (T - 1)(T - 3)(T - 9)(T - 4)(T - 5)$ over $\mathbb{Z}/(11)$. The minimal polynomial of a non-trivial T will either be one of the 4 linear factors other than $(T - 1)$, or it will be a product of two distinct linear factors, of which there are 10 possibilities. So there are 14 conjugate classes, all represented by diagonal matrices and classified by an unordered pair of eigenvalues. However, T, T^2, T^3, and T^4 all define isomorphic semidirect product groups, by using the $\mathrm{Aut}(\mathbb{Z}/(5)) = \mathrm{Aut}(H)$ action. All 14 conjugate classes fall into 4 distinct diagonal subgroups, which are easy to write out by simply taking powers of various diagonal matrices. Thus there are 4 distinct $\mathrm{Aut}(H) \times \mathrm{Aut}(K)$ orbits and 4 distinct non-abelian semidirect products.

Looking more closely at the above example, $\mathbb{Z}/(5) \times \mathbb{Z}/(5)$ actually has 6 distinct subgroups of order 5. But, for example, the subgroup generated by diagonal matrices $(3,5)$ and $(5,3)$ are conjugate in $GL(2,\mathbb{Z}/(11))$. In three of the four non-conjugate diagonal subgroups the four powers of T represent distinct conjugate classes. In the fourth, generated by diagonal matrix $T = (3,4)$, one has $T^2 = (9,5)$, $T^3 = (5,9)$, and $T^4 = (4,3)$, so there are only two distinct conjugate classes in this subgroup. This example illustrates a comment made above about non-cyclic Sylow subgroups in $GL(n,\mathbb{Z}/(q)) = \mathrm{Aut}(K)$. In this case we have the Sylow subgroup $\mathbb{Z}/(5) \times \mathbb{Z}/(5) \subset GL(2,\mathbb{Z}/(11))$. Just conjugating in $\mathrm{Aut}(K)$ to get $u : \mathbb{Z}/(5) \to \mathbb{Z}/(5) \times \mathbb{Z}/(5)$ doesn't reduce the classification of orbits to (non-trivial) $\mathrm{Aut}(\mathbb{Z}/(5))$ orbits in $\mathrm{Hom}(\mathbb{Z}/(5), \mathbb{Z}/(5) \times \mathbb{Z}/(5))$, of which there would be 6. There is still $\mathrm{Aut}(K)$ conjugation going on inside the $\mathbb{Z}/(5) \times \mathbb{Z}/(5)$. Linear algebra does come to the rescue and leads to the complete classification of semidirect products of $(\mathbb{Z}/(11))^2$ by $\mathbb{Z}/(5)$.

Suppose now, to up the ante, that H is a little more complicated than a cyclic group or a $\mathbb{Z}/(p)$-vector space. The next simplest groups are probably the groups $H = \mathbb{Z}/(p^2) \times \mathbb{Z}/(p)$. It is not so hard to show $|\mathrm{Aut}(H)| = p^3(p-1)^2$. You choose generators x and y of H of order p^2 and p, respectively. An automorphism a must take x to an element of order p^2, of which there are $p^3 - p^2$ choices. Then y must go to an element of order p not in $a(\langle x \rangle)$, of which there are $p^2 - p$ choices. For $H = \mathbb{Z}/(4) \times \mathbb{Z}/(2)$, the automorphism group turns out to be the dihedral group of order 8.

Sometimes you can determine $\mathrm{Aut}(H) \times \mathrm{Aut}(K)$ orbits in $\mathrm{Hom}(H, \mathrm{Aut}(K))$ without requiring the actual structure of $\mathrm{Aut}(H)$. For example, suppose $H = \mathbb{Z}/(p^2) \times \mathbb{Z}/(p)$, and you get to a situation of just needing to understand $\mathrm{Aut}(H)$ orbits of maps $u : H \to A$, where A is abelian. Distinct image groups in A definitely implies different orbits. Non-isomorphic kernel groups in H definitely implies different orbits. If the image $u(H)$ is $\mathbb{Z}/(p^2) \times \mathbb{Z}/(p)$ or $\mathbb{Z}/(p^2)$, thinking about how you can move generators x and y around by an automorphism, as described in the above paragraph, pretty quickly shows there is exactly one orbit with this fixed image group. If $u(H) = \mathbb{Z}/(p)$, there are two possible isomorphism types of kernels, $\mathbb{Z}/(p) \times \mathbb{Z}/(p)$ and $\mathbb{Z}/(p^2)$. Again, pushing generators x and y of H around, you can see there is one orbit for each kernel type, or two non-trivial orbits with this fixed image group. But if $u(H) = \mathbb{Z}/(p) \times \mathbb{Z}/(p)$, so $\ker u$ is unambiguously the subgroup pH, then rather remarkably there are still two distinct non-trivial $\mathrm{Aut}(H)$ orbits with this fixed image group and fixed kernel. This is pretty tricky, and marks kind of a boundary of what you have any chance of explicitly carrying out.

If you want to try out your skills, using the above ideas, classify all groups of order 1144 that have an abelian 2-Sylow subgroup.

If H is non-abelian, determining $\mathrm{Aut}(H)$, or even its order, can be formidable. If you want to have more fun, determine the automorphism groups of all the groups of order 8. Then classify all groups of order 56. This can be done. Another fun problem is to determine the automorphism group of the non-abelian group of order pq, where p and q are primes and $q = 1 \bmod p$. This would seem relevant for finding all groups of order pqr, where $p < q < r$ are primes, since in any such group the r-Sylow subgroup is normal.