Lecture 10-2: Simple groups of order 60 and 168; finite abelian groups

October 2, 2024

Last time I used Sylow's Theorem to show that groups whose order is product of two distinct primes are semidirect products, so that in particular they are always nonsimple (i.e. they have nontrivial normal subgroups). One can also use this theorem to study simple groups. Today, following Chapter 6 in the text, I will be analyzing simple groups of order 60 or 168 (these being the two smallest nonprime orders of simple groups). I will also give a classification of finite abelian groups (which will be generalized to a much larger class of groups next term)

Recall from last week that there are seven conjugacy classes in the symmetric group S_5, having orders $24, 30, 20, 20, 15, 10$, and 1, and represented respectively by a 5-cycle, a 4-cycle, the product of disjoint 3- and 2-cycles, a 3-cycle, the product of two disjoint 2-cycles, a single 2-cycle, and the identity. The first, fourth, fifth, and seventh of these classes lie in the alternating group A_5, while the others are disjoint from it; the first class splits up into two disjoint A_5-conjugacy classes, both of size 12, while the others form single A_5-conjugacy classes. Since a normal subgroup of A_5 must be a union of conjugacy classes closed under the product, one checks easily that A_5 is simple (Corollary 22, p. 145), using much the same argument as the one used last week to show that A_5 is the only subgroup of S_5 of order 60.

Using the Sylow Theorem, we can now show:

Proposition 23, p. 145

Any simple group of order 60 is isomorphic to A_5.

.

Proof.

Let G be a simple group of order 60. The number n_5 of 5-Sylow subgroups cannot be 1 and divides 6, so must be exactly 6. The conjugation action of G on the set of its 5-Sylow subgroups has trivial kernel, since G is simple, so realizes G as (isomorphic to) a subgroup of S_6. The intersection of G and A_6 is then either all of G or of index two; since G is simple, it must be all of G. Hence G embeds in A_6 as a subgroup of index 6. The left action of G on the left cosets of this subgroup fixes the identity coset and permutes the other 5. If it did so trivially, then G would be a normal subgroup of A_6. There is an element $g \in G$ of order 5 (generating a 5-Sylow subgroup), which must be a 5-cycle in A_6, say (12345) (fixing the index 6). G would then contain the subgroup generated by all S-conjugates of powers of g. □

Proof.

This is all of S, since S identifies with A_5 and the latter group is simple; so we would have $G = S$. But S is not normal in A_6, a contradiction, so G is not normal in A_6. Then its action on its left cosets other than itself in A_6 is not trivial, whence G is isomorphic to a subgroup of the permutation group S_5 of these cosets. This forces $G \cong A_5$, as desired. □

Now let G be simple of order 168. It turns out that there is only one possibility for G up to isomorphism. I will not prove this (this is done in the text on pages 207 to 211), but I will explicitly construct G and indicate its close relationship to the field $\mathbb{Z}_2$ with two elements. Recall first that $\mathbb{Z}_2$ is indeed a field under addition and multiplication, as is $\mathbb{Z}_p$ for any prime p (see p. 34); when regarding $\mathbb{Z}_2$ as a field I will denote it by F_2 to emphasize the field structure.

Start with $V = F_2^3$, the three-dimensional vector space of ordered triples over F_2. This space has exactly seven lines through the origin, one for each of its nonzero vectors, and likewise seven planes through the origin. Note that every pair of distinct such lines spans a unique such plane and likewise every pair of distinct such planes intersects in a unique line. Thus lines and planes in this setting exhibit a more uniform behavior than points and lines in $\mathbb{R}^2$, where there is a unique line passing through any pair of points but a pair of lines fails to intersect in a point if the lines are parallel.

Now look at the group $G = GL_3(F_2)$ of invertible 3×3 matrices with entries in the field F_2. In homework for this week you will show that the order of G is $7 \cdot 6 \cdot 4 = 168$. G acts transitively on the lines through the origin or planes through the origin in V; if a line ℓ is contained in such a plane P, then $g\ell$ is contained in gP. Note also that every plane P is the union of exactly three lines ℓ. This situation is famously depicted by the Fano plane (see p. 210), in which the vertices represent lines and the lines, together with the circle, represent planes.

More generally, if F_q denotes the finite field of order q, which turns out to be unique up to isomorphism whenever it exists and exists if and only if $q = p^k$ is a power of a prime p, then the projective plane $\mathbb{P}^2_q$, consisting of all lines through the origin in the vector space F_q^3, has $\frac{q^3-1}{q-1} = q^2 + q + 1$ elements. Every plane containing the origin in F_q^3 is the union of $q + 1$ lines in $\mathbb{P}^2_q$, any two of them intersecting only at the origin when viewed as lines in $V = F_q^3$. The group $GL_3(F_q)$ of 3×3 invertible matrices over F_q acts transitively on $\mathbb{P}^2_q$ and on the set of planes through the origin in V.

This group is a simple group, as is the group $GL_n(F_q)$ of invertible $n \times n$ matrices over F_q for any $n \geq 3$ (and in fact for $n = 2$ as well, provided that $q \geq 5$)).

Returning to the setting of a simple group of order 168, it turns out that the 2-Sylow subgroups of any such group are dihedral of order 8 and each has exactly two conjugacy classes of subgroups isomorphic to the Klein 4-group, generated by the center of the dihedral group together with a representative of one of its two conjugacy classes of reflections. The normalizer of any of these Klein 4-groups is isomorphic to the symmetric group S_4, so that there are $168/24 = 7$ distinct conjugates of any of them.

If U, W are two nonconjugate copies of the Klein four-group in any fixed 2-Sylow subgroup of G, then identify the conjugates of U with points in the Fano plane and the conjugates of W with lines in this plane. Decree that the point corresponding to a conjugate U' of U lies in the line corresponding to a conjugate W' of W if and only if U' and W' generate a Sylow 2-subgroup of G, we can use the action of G on such points and lines to identify G with $GL_3(F_2)$.

Having gotten just this little tase of the rich interplay between finite groups, finite fields, and geometry, we now turn to the abstract setting of an arbitrary finite abelian group A. For every p dividing the order $|A|$ of A, the p-Sylow subgroup A_p is unique and normal in A; by counting elements we see that A is the direct product of its Sylow subgroups A_p. In order to classify such groups A it therefore suffices to classify abelian p-groups for a fixed prime p.

The surprisingly neat result is that any abelian p-group is the direct product of cyclic p-groups. I prove this for groups P of order p^n by induction on n, following the argument on pp. 196-7 of the text. I know that any such P admits a normal subgroup Q of order p^{n-1}, which I can assume inductively is the direct product $C_1 \times \cdots \times C_m$ of cyclic groups C_i with C_i of order p^{n_i}, arranged so that $n_1 \geq \ldots \geq n_m$. The quotient P/Q is cyclic of order p; choosing $y \in P, y \notin Q$ I then have $y^p \in Q$. Now an element g of a cyclic p-group G generates G if and only if it is not the pth power of another element. Replacing y by a suitable translate yz for some $z \in C_i$ whenever the projection y_i of y^p is a pth power in C_i, I may assume that for every i that either this projection y_i is 1 or else it generates C_i.

If $y_i = 1$ for all i then it is easy to see that P is the direct product of Q and the cyclic subgroup $Y = \langle y \rangle$ generated by y. Otherwise choose the least i such that y_i generates C_i, so that the order of Y is p^{n_i+1}. Then I claim that P is the direct product of Y and the C_j for $j \neq i$. Indeed, it is clear from the construction that the intersection of Y and the product P' of these C_j is trivial, whence by counting elements we see that $P' \times Y$ fills out P, as desired.

As an immediate consequence we get

Theorem 5, p. 161

Any finite abelian group A is the direct product of cyclic subgroups of prime-power order.

Given A and a fixed power p^m of a prime p, by counting elements a of A with $a^{p^m} = 1$, one sees that the number of cyclic factors of A of order p^m is determined uniquely by A (see Theorem 5 (3), p. 161). In particular, any finite abelian group of order p^n is a direct product of cyclic groups of orders n_i, where $\sum n_i = n$, with two such products isomorphic if and only if their factors (after a permutation) have the same orders. Any *unordered* collection of positive integers n_i with $\sum n_i = n$ is called a partition of n. It follows that up to isomorphism, the number of abelian groups of order p^n equals the number of partitions of n. For example, there are five partitions of 4, namely $4, 3+1, 2+2, 2+1+1, 1+1+1+1$, and accordingly five isomorphism classes of abelian groups of order p^4 for any prime p.

I close by proving a property mentioned earlier about automorphisms. Let A be a finite subgroup of the multiplicative group K^* of a field K. As a finite abelian group, A is the direct product of its p-Sylow subgroups A_p. But now a basic fact about polynomials over fields is that a polynomial over a field K with degree n has at most n roots in K (Proposition 17, p. 313), so for every k there are at most p^k elements of A_p of order dividing p^k.

Since A_p is a direct product of cyclic p-groups, it must in fact be a single cyclic group; since the direct product of cyclic groups of relatively prime orders is again cyclic, we see that A must be cyclic in this situation (Proposition 18, p. 314). In particular, the multiplicative group F_p^* of the finite field of order p is cyclic of order $p-1$ (Corollary 19, p. 314). Now an automorphism ϕ of F_p, regarded just as an additive group, is determined by the image $\phi(1)$ of its generator 1, which can be any nonzero element of F_p. The composite $\phi \circ \psi$ of two such automorphisms sends 1 to the product $\phi(1)\psi(1)$, so that the automorphism group $\mathrm{Aut}\, F_p \cong F_p^* \cong \mathbb{Z}_{p-1}$, as claimed earlier.