

8. WHAT WE DIDN'T DO

In this section we will discuss some topics that will not be covered in class but that are necessary for certain purposes (e.g., the Master's Exam — but this is *not* a complete list of topics you need for the Master's Exam, nor is it a list of topics that will definitely appear on the exam).

8.1. The Sylow Theorems. Lagrange's Theorem tells us that if H is a subgroup of G , then $|H|$ divides $|G|$. The converse is not usually true. For example, A_4 is a group of order 12 with no subgroup of order 6. However, there are two cases where there is a converse. The first result can be proved directly, but it also follows from the Fundamental Theorem of Abelian groups. The second result, the Sylow Theorems, is a major result in finite group theory. It has many applications to studying groups of small order, and hence is a favorite in creating problems. We give some applications after the theorem.

Proposition (Converse to Lagrange's Theorem for Abelian Groups). *Let G be an Abelian group with n elements. If m is a positive integer that divides n , then G has a subgroup with m elements.*

Theorem (The Sylow Theorems). *Let G be a finite group whose order is divisible by a prime number p and suppose that p^n is the highest power of p that divides $|G|$. Then the following statements are true.*

- (1) *If $0 \leq i \leq n$, then G has a subgroup of order p^i .*
- (2) *All subgroups of G of order p^n are conjugate. (That is, if P, P' are subgroups of order p^n , there is a $g \in G$ with $gPg^{-1} = P'$).*
- (3) *G contains a normal subgroup of order p^n if and only if G contains exactly 1 subgroup of order p^n .*
- (4) *Let d be the number of subgroups of G of order p^n .*

Then $d \mid |G|$ and $d \equiv 1 \pmod{p}$.

We can actually be more precise. If P is any subgroup of G of order p^n and $N_G(P) = \{g \in G \mid gPg^{-1} = P\}$, then $d = [G : N_G(P)]$. In particular, this implies that $d \mid |G|/p^n$.

Remark. When p^n is the largest power of p that divides $|G|$, we call a subgroup of G of order p^n a p -Sylow subgroup of G , or simply a Sylow subgroup of G .

Example. Here are some examples of the use of the Sylow Theorems.

(1) Let G be a group of order $20 = 2^2 \cdot 5$. By the Sylow Theorems, G has a subgroup P of order 5. Moreover, if d is the number of such subgroups, we have $d \mid 20$ and $p \equiv 1 \pmod{5}$. Thus the possible values for d are 1, 6, 11, 16, 21, \dots . Only $d = 1$ divides 20, so we must have $d = 1$. [If we used the improved bound in the Sylow Theorem, we can actually say $d \mid (20/5 = 4)$ and cut down the values of d we have to check.] Hence there is only one subgroup of G of order 5. By the Sylow Theorems again, this implies the subgroup P is normal. Thus by a pure counting argument, we have shown every group of 20 elements contains a normal subgroup with 5 elements.

What else do the Sylow Theorems tell us about G ? The number of subgroups of order 4 divides 20; actually it divides $20/4 = 5$. Moreover, it is congruent to 1 mod 2, i.e., it is odd. Thus there are either 1 or 5 subgroups of order 4. If there is only one, it is normal. One can then show that G must be Abelian — see the next example. It is also possible to have 5 subgroups of order 4: the group $D_5 \times \mathbb{Z}_2$ is an example of such a group.

(2) Let G be a group of order $35 = 5 \cdot 7$. Using arguments like those in (1), we conclude that G must have a normal subgroup N of order 5 and another normal subgroup K of order 7. By Lagrange's Theorem, $N \cap K$ can only have 1 element, so $N \cap K = \{e\}$. A fairly simple counting argument shows that in this case, the set $NK = \{nk \mid n \in N, k \in K\}$

has $|N||K| = 35$ elements. Thus $G = NK$. Using this equality, the equality $N \cap K = \{e\}$, and the fact that N, K are both normal, we can show that the map $N \times K \rightarrow G$ defined by $(n, k) \mapsto nk$ is a group isomorphism. Thus $G \cong N \times K$.

In our case, we know what N and K are: $N \cong \mathbb{Z}_5$ and $K \cong \mathbb{Z}_7$, so $G \cong \mathbb{Z}_5 \times \mathbb{Z}_7 \cong \mathbb{Z}_{35}$. Thus every group with 35 elements is isomorphic to \mathbb{Z}_{35} .

(3) The general case of example (2) is the following result. See if you can prove it: if p, q are prime numbers such that $p < q$ and $p \nmid q - 1$, every group of order pq is isomorphic to \mathbb{Z}_{pq} (and so is cyclic).

Actually the above result is “iff”, though we don’t have the tools to prove the other direction. That is, if $p < q$ are primes and $p \mid q - 1$, there is a non-Abelian group of order pq .

(4) Here is a trickier example. First a note: if G contains a normal subgroup N , then we can sort of break down G into N and G/N . Thus in some sense the building blocks of group theory are groups with no normal subgroups except $\{e\}$ and G . Such groups are called *simple*. The simple Abelian groups are the groups \mathbb{Z}_p where p is prime, so the question to solve is “What are the non-Abelian simple groups?”. The group A_5 is a simple group of order 60. Using the Sylow Theorems and other results we’ve seen (such as the fact that a group of order p^n has a non-trivial center and so cannot be simple), plus counting arguments, one can show that no non-Abelian group of order less than 60 is simple. Here’s one example.

Let G be a group of $56 = 2^3 \cdot 7$ elements. The usual counting argument from the Sylow Theorems tells us that G has either 1 or 7 subgroups of order 8 and either 1 or 8 subgroups of order 7. We want to show that one of these numbers is 1.

Suppose that the Sylow subgroups of order 7 are not normal: this means there must be 8 of them. If P, Q are different Sylow subgroups of order 7, Lagrange’s Theorem tells us that $P \cap Q = \{e\}$. Thus each 7-Sylow subgroup contributes 6 unique elements to G , plus e . This means G has 48 elements of order 7. But G has at least 1 subgroup of order 8, and we have used up all but 8 of the elements of G . Thus the remaining elements of G are only enough to form 1 subgroup of order 8. (Make sure you understand this: assume G has ≥ 2 subgroups of order 8 and get a contradiction.) Thus by the Sylow Theorems, G contains a normal subgroup of order 8.

Examine the above proof carefully. We did not show that G has a normal subgroup of order 8 and we did not show it has a normal subgroup of order 7. We showed it has at least one or the other, but we don’t know which one. In fact, everything is possible: there are groups of 56 elements with (a) normal subgroups of 7 and 8 elements; (b) a normal subgroup of 7 elements but not one of 8; (c) a normal subgroup of 8 elements but not one of 7.

See Artin §6.4 for more; look at the problems from that section for more as well.

8.2. The Structure of Permutations. Recall that a permutation $\sigma \in S_n$ is a *k-cycle* if there are distinct numbers $a_1, \dots, a_k \in \{1, 2, \dots, n\}$ such that $\sigma(a_i) = a_{i+1}$ for $1 \leq i \leq k - 1$, $\sigma(a_k) = a_1$, and $\sigma(j) = j$ if $j \in \{1, 2, \dots, n\} \setminus \{a_1, \dots, a_k\}$. We write $\sigma = (a_1 a_2 \dots a_k)$ and we call k the *length* of the cycle. We say a cycle is *non-trivial* if its length is at least 2. It is a good exercise to show that any two cycles of the same length are conjugate.

Cycles $\sigma_1, \dots, \sigma_r \in S_n$ are said to be *disjoint* if there is no number j with $1 \leq j \leq n$ such that $\sigma_i(j) \neq j$ for two or more values of i . That is, cycles are disjoint if every number between 1 and n is moved by at most one of the cycles. Note that disjoint cycles commute with each other.

Theorem (Decomposition of Permutations into Cycles). *Let $\sigma \in S_n$.*

- (1) *There are disjoint non-trivial cycles $\sigma_1, \dots, \sigma_r$ such that σ is the product $\sigma_1 \circ \dots \circ \sigma_r$. (The product is the same in any order.)*
- (2) *The cycles $\sigma_1, \dots, \sigma_r$ in (1) are unique up to order (always assuming they are all non-trivial).*
- (3) *If $\sigma' \in S_n$, then σ and σ' are conjugate if and only if they have the same cycle structure, that is if and only if the decompositions of σ, σ' into disjoint non-trivial cycles involve the same number of cycles of each length.*

For example, the permutations $(1\ 2\ 3)(4\ 5\ 6)(7\ 8)$, $(4\ 10\ 5)(3\ 6)(9\ 2\ 8)$, $(5\ 8)(3\ 4)(4\ 2)(6\ 9\ 1)$ in S_{12} are all conjugate. (It is necessary to multiply the non-disjoint cycles in the third permutation and get a decomposition into *disjoint* cycles to verify that this permutation is conjugate to the other two.)

See Artin §6.6 and its problems for more.

8.3. The Fundamental Theorem of Abelian Groups. The “ultimate” goal of finite group theory would be to classify all finite groups, that is, give a complete list of finite groups and give a way to tell which group on the list a given group is isomorphic to. It is very unlikely this goal will be realized anytime soon. However, there is a complete classification of finite Abelian groups, which we state next. There are two versions: both say that every Abelian group is isomorphic to a finite product of cyclic groups; they differ in which cyclic groups are used.

Recall that for Abelian groups G_1, \dots, G_n , the Cartesian product is usually written with \oplus , so $\oplus_{i=1}^n G_i = G_1 \times \dots \times G_n$, and we call this the *direct sum* of G_1, \dots, G_n .

Theorem (Fundamental Theorem of Finite Abelian Groups, version 1). *Let G be a finite Abelian group. Then G is isomorphic to a finite direct sum of cyclic groups of prime power order (that is, cyclic groups of order p^m for primes p and positive integers m). Moreover, the number of cyclic factors and their sizes is unique.*

Another way to say this: $G \cong \oplus_{i=1}^k \mathbb{Z}_{p_i^{m_i}}$ for some primes p_1, \dots, p_k (possibly containing repeats) and positive integers m_i . Moreover, k and the numbers $p_i^{m_i}$ are unique (up to order).

The numbers $p_i^{m_i}$ that occur are called the *elementary divisors* of G .

Theorem (Fundamental Theorem of Finite Abelian Groups, version 2). *Let G be a finite Abelian group. Then there are unique integers d_1, \dots, d_r greater than 2 such that $d_1 \mid d_2 \mid \dots \mid d_r$ and $G \cong \oplus_{i=1}^r \mathbb{Z}_{d_i}$.*

The numbers d_1, \dots, d_r are called the *invariant factors* of G .

There are several proofs of this result. The reason for the two versions can be seen from a simple example like $G = \mathbb{Z}_{12}$. Since this is cyclic, it fits the pattern of version 2 of the Fundamental Theorem with $r = 1$, $d_1 = 12$. On the other hand, since $\gcd(3, 4) = 1$, we know that $\mathbb{Z}_{12} \cong \mathbb{Z}_3 \oplus \mathbb{Z}_4$. This fits the pattern of version 1 of the Fundamental Theorem with $k = 2$ and elementary divisors $3, 4 = 2^2$.

Here is a sample application of the Fundamental Theorem. Let us list all Abelian groups of order $504 = 2^3 \cdot 3^2 \cdot 7$. Using version 1, we see that we must figure out the various ways of writing 2^3 and 3^2 as products, and combine them. This leads to the following list, which contains exactly one from each isomorphism class of Abelian groups of order 504.

$$\begin{aligned} &\mathbb{Z}_{2^3} \oplus \mathbb{Z}_{3^2} \oplus \mathbb{Z}_7; & \mathbb{Z}_{2^2} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{3^2} \oplus \mathbb{Z}_7; & \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{3^2} \oplus \mathbb{Z}_7; \\ &\mathbb{Z}_{2^3} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7; & \mathbb{Z}_{2^2} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7; & \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7. \end{aligned}$$

Thus there are 6 different groups.

If we use version 2, we get the following list. The groups in this list are isomorphic to the groups in the first list, in the given order.

$$\mathbb{Z}_{504}; \quad \mathbb{Z}_2 \oplus \mathbb{Z}_{252}; \quad \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{126}; \quad \mathbb{Z}_3 \oplus \mathbb{Z}_{168}; \quad \mathbb{Z}_6 \oplus \mathbb{Z}_{84}; \quad \mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_{42}.$$

As an exercise, you might think about how to show there are 25 (non-isomorphic) Abelian groups of order 10,000 without actually writing them out. (And 121 of order 1,000,000.)

See Artin §12.6 and its problems for more.

8.4. Polynomial and Canonical Forms for Matrices. At the beginning of the semester we saw that for any matrix $A \in M_n(\mathbb{C})$, there is a unitary matrix $P \in GL_n(\mathbb{C})$ such that PAP^{-1} is upper triangular. If we allow an arbitrary $P \in GL_n(\mathbb{C})$, we can make PAP^{-1} very upper triangular: we can get every entry not on the main diagonal or immediately above the main diagonal to be 0. The resulting form is called *Jordan form*. (Note: Artin uses lower triangular instead of upper triangular matrices, so his results are the transpose of ours.)

One can prove this by first generalizing the Fundamental Theorem of Finite Abelian groups to a Fundamental Theorem of “Finite” Modules over a Euclidean Domain or over a PID. (Abelian groups are just \mathbb{Z} -modules.) “Finite” is in quotes because we need to replace it with an analogous (but weaker and more complicated) condition. After this, one shows how to make a matrix in $M_n(F)$ correspond to a finite-dimensional module over $F[x]$, and then one applies the generalized Fundamental Theorem. We will not give the details.

To state the theorem, we need to introduce some notation. Let F be a field and let $c \in F$. A *Jordan block* of size k with eigenvalue c is the matrix $J = J(k, c)$ with each diagonal entry equal to c , each entry just above the diagonal equal to 1, and every other entry equal to 0. For example,

$$J(4, c) = \begin{pmatrix} c & 1 & 0 & 0 \\ 0 & c & 1 & 0 \\ 0 & 0 & c & 1 \\ 0 & 0 & 0 & c \end{pmatrix}.$$

We say a matrix A is in *block Jordan form* if

$$(*) \quad A = \begin{pmatrix} J(k_1, c_1) & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & J(k_2, c_2) & \mathbf{0} & \mathbf{0} \\ \vdots & & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & J(k_r, c_r) \end{pmatrix},$$

for some Jordan blocks $J(k_1, c_1), \dots, J(k_r, c_r)$.

An example of a matrix in block Jordan form is

$$\begin{pmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

(Note: when we define them below, come back and calculate the characteristic and minimal polynomials of the matrix just given. They are $(x-2)^3(x-1)$ and $(x-2)^2(x-1)$ respectively.)

The theorem we seek is the following.

Theorem (Jordan Canonical Form). *Let F be an algebraically closed field (e.g., $F = \mathbb{C}$) and let $A \in M_n(F)$. Then there exists a $P \in GL_n(F)$ such that PAP^{-1} is in block Jordan form. Moreover, the Jordan blocks that occur in block Jordan form are unique up to order.*

The uniqueness statement means that if QAQ^{-1} is also in block Jordan form, the same Jordan blocks (same eigenvalues and same sizes) occur, but possibly in a different order. In fact, by appropriately choosing Q , we can re-arrange the Jordan blocks into any order we desire. Note that there is no requirement that the c_i and k_i be distinct: it is possible that $c_i = c_j$ even if $i \neq j$ and that $k_i = k_j$ even if $i \neq j$.

There are algorithms for computing Jordan form and the matrix P (assuming one can find the roots of the characteristic polynomial, which gives the eigenvalues). However, we can often deduce a lot about the Jordan form without explicitly computing it. For example, since A and PAP^{-1} are similar, they have the same characteristic polynomial $\det(xI - A)$ and the same eigenvalues.

The Jordan block $J(k, c)$ has characteristic polynomial $(x - c)^k$ and its only eigenvalue is c . Thus if PAP^{-1} is in the block Jordan form given by the equation (*), the characteristic polynomial of A is $\prod_{i=1}^r (x - c_i)^{k_i}$. Moreover, the set $\{c_1, \dots, c_r\}$ (which may contain repetition) is the set of eigenvalues of A .

If we look a little more closely at the Jordan blocks, we see that each contributes one linearly independent eigenvector. Thus the number of Jordan blocks is the (maximum) number of linearly independent eigenvectors of A .

Let's turn the above discussion around: suppose $f(x)$ is the characteristic polynomial of A . Since F is algebraically closed, we can factor it into linear factors. If c is an eigenvalue of A , then f has $(x - c)^k$ as a factor for some maximum $k \geq 1$. Using the formula above for the characteristic polynomial of PAP^{-1} , we see that k equals the sum of the sizes of all Jordan blocks with eigenvalue c .

Suppose for example that A is a 4×4 complex matrix with characteristic polynomial $f(x) = (x - 2)^3(x - 1)$. Then the Jordan form of A must contain Jordan blocks with eigenvalues 2 and 1, and the sizes of the Jordan blocks with eigenvalue 2 must add up to 3. Thus there are three possible Jordan forms for A :

$$B = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad C = \begin{pmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad D = \begin{pmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

If we know how many linearly independent eigenvectors A has with eigenvalue 2 (that is, if we know the dimension of the nullspace of $2I - A$), we can determine which of B, C, D is the Jordan form. (If $n(2I - A) = 3, 2, 1$, then the Jordan form is B, C, D respectively.)

There is another way in which one can sometimes determine the Jordan form of A . Let us continue with the above example. If we consider the polynomial $b(x) = (x - 2)(x - 1)$, $c(x) = (x - 2)^2(x - 1)$, $d(x) = (x - 2)^3(x - 1)$, then $b(B) = c(B) = d(B) = 0$, while $b(C) \neq 0 = c(C) = d(C)$ and $b(D), c(D) \neq 0 = d(D)$. Since $g(PAP^{-1}) = Pg(A)P^{-1}$ for any polynomial g , we see that $g(A) = 0$ iff $g(PAP^{-1}) = 0$. Thus by substituting our matrix A into $b(x), c(x), d(x)$, we can tell which of B, C, D is the Jordan form of A . We are not always so lucky, but frequently we are. The next two results formalize some of this discussion.

Theorem (Cayley-Hamilton Theorem). *Let F be a field, let $A \in M_n(F)$, and let $f(x) = \det(xI - A)$ be the (monic) characteristic polynomial of A . Then $f(A) = 0$.*

Theorem (Minimal Polynomial). *Let F be a field and let $A \in M_n(F)$. Then there is a unique monic polynomial $p(x) \in F[x]$ of smallest degree with $p(A) = 0$. We have $\deg p \leq n$ and p divides the characteristic polynomial of A .*

*In fact, p is the unique monic polynomial in $F[x]$ with the following properties:
(a) $p(A) = 0$ and (b) for any $q \in F[x]$ with $q(A) = 0$, we have $p \mid q$.*

In the example just before the theorems, b, c, d are the minimal polynomials of B, C, D respectively. Thus we can determine the Jordan form of A from its minimal and characteristic polynomials in this case. This is not always true, unfortunately.

One can prove that every eigenvalue of A is a root of its minimal polynomial, and we saw that the minimal polynomial is a factor of the characteristic polynomial. There is generally no simple formula for the minimal polynomial of a matrix.

If we put all of our results together, we can add information to the Jordan form theorem as follows.

Theorem (Jordan Canonical Form). *Let F be an algebraically closed field (e.g., $F = \mathbb{C}$) and let $A \in M_n(F)$. Then there exists a $P \in GL_n(F)$ such that PAP^{-1} is in block Jordan form. Moreover, the Jordan blocks that occur in block Jordan form are unique up to order.*

In addition, the number of Jordan blocks with eigenvalue c is equal to $n(cI - A)$ (the dimension of the nullspace of $cI - A$). The size of the largest Jordan block with eigenvalue c is equal to the largest exponent d such that $(x - c)^d$ divides the minimal polynomial of A .

Example. Here are some examples. Assume we are working over \mathbb{C} .

- (1) Suppose A is a 5×5 matrix with characteristic polynomial $x^5 - x^3$ and minimal polynomial $x^4 - x^2$. Find the Jordan form of A — it is determined.
- (2) Write down a matrix in Jordan form with characteristic polynomial $(x - 1)^4(x + 1)$ and minimal polynomial $(x - 1)^2(x + 1)$. There are two possibilities.

See Artin §12.7 and its problems for more.

8.5. Finite Fields.

Theorem (Classification of Finite Fields). *Let q be a positive integer. Then there is a field with q elements if and only if there is a prime number p and a positive integer n such that $q = p^n$. When q is of this form, there is exactly one field with q elements (up to isomorphism), which we denote by \mathbb{F}_q . Thus $\mathbb{F}_p = \mathbb{Z}_p$.*

The elements of \mathbb{F}_q are all roots of the polynomial $x^q - x$.

See Artin §13.6 and its problems for more.

INDEX OF DEFINITIONS

p -Sylow subgroup, 1
block Jordan form, 4
cycle, 2
cycle structure, 3
direct sum, 3
disjoint, 2
elementary divisors, 3
invariant factors, 3
Jordan block, 4
Jordan form, 4
length, 2
non-trivial, 2
simple, 2
Sylow subgroup, 1