has more than one Sylow p-subgroup and that any two distinct Sylow p-subgroups of $N_G(P \cap Q)$ intersect in the subgroup $P \cap Q$. (Thus $|N_G(P \cap Q)|$ is divisible by $p \cdot |P \cap Q|$ and by some prime other than p. Note that Sylow p-subgroups of $N_G(P \cap Q)$ need not be Sylow in G.)

14. Prove that there are no simple groups of order 144, 525, 2025 or 3159.

General exercises:

15. Classify groups of order 105.

16. Prove that there are no non-abelian simple groups of odd order < 10000.

17. **(a)** Prove that there is no simple group of order 420.
(b) Prove that there are no simple groups of even order < 500 except for orders 2, 60, 168 and 360.

18. Prove that if G is a group of order 36 then G has either a normal Sylow 2-subgroup or a normal Sylow 3-subgroup.

19. Show that a group of order 12 with no subgroup of order 6 is isomorphic to A_4.

20. Show that a group of order 24 with no element of order 6 is isomorphic to S_4.

21. Generalize Lemma 13 by proving that if $n_p \not\equiv 1 (\text{mod } p^k)$ then there are distinct Sylow p-subgroups P and R of G such that $P \cap R$ is of index $\leq p^{k-1}$ in both P and R.

22. Suppose over all pairs of distinct Sylow p-subgroups of G, P and R are chosen with $|P \cap R|$ maximal. Prove that $N_G(P \cap R)$ is not a p-group.

23. Let A and B be normal subsets of a Sylow p-subgroup P of G. Prove that if A and B are conjugate in G then they are conjugate in $N_G(P)$.

24. Let G be a group of order pqr where p, q and r are primes with $p < q < r$. Prove that a Sylow r-subgroup of G is normal.

25. Let G be a simple group of order p^2qr where p, q and r are primes. Prove that $|G| = 60$.

26. Prove or construct a counterexample to the assertion: if G is a group of order 168 with more than one Sylow 7-subgroup then G is simple.

27. Show that if $\mathcal{F}$ is any set of points and lines satisfying properties (11) to (13) in the subsection on simple groups of order 168 then the graph of incidences for $\mathcal{F}$ is uniquely determined and is the same as Figure 1 (up to relabeling points and lines). [Take a line and any point not on this line. Depict the line as the base of an equilateral triangle and the point as the vertex of this triangle not on the base. Use the axioms to show that the incidences of the remaining points and lines are then uniquely determined as in Figure 1.]

28. Let G be a simple group of order $3^3 \cdot 7 \cdot 13 \cdot 409$. Compute all permissible values of n_p for each $p \in \{3, 7, 13, 409\}$ and reduce to the case where there is a unique possible value for each n_p.

29. Given the information on the Sylow numbers for a hypothetical simple group of order $3^3 \cdot 7 \cdot 13 \cdot 409$, prove that there is no such group. [Work with the permutation representation of degree 819.]

30. Suppose G is a simple group of order 720. Find as many properties of G as you can (Sylow numbers, isomorphism type of Sylow subgroups, conjugacy classes, etc.). Is there such a group?

6.3 A WORD ON FREE GROUPS

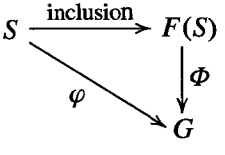
In this section we introduce the basic theory of so-called free groups. This will enable us to make precise the notions of generators and relations which were used in earlier chapters. The results of this section rely only on the basic theory of homomorphisms.

The basic idea of a free group $F(S)$ generated by a set S is that there are no relations satisfied by any of the elements in S (S is "free" of relations). For example, if S is the set $\{a, b\}$ then the elements of the free group on the two generators a and b are of the form a, aa, ab, $abab$, bab, etc., called *words* in a and b, together with the inverses of these elements, and all these elements are considered distinct. If we group like terms together, then we obtain elements of the familiar form a, b^{-3}, $aba^{-1}b^2$ etc. Such elements are multiplied by concatenating their words (for example, the product of aba and $b^{-1}a^3b$ would simply be $abab^{-1}a^3b$). It is natural at the outset (even before we know S is contained in some group) to simply *define* $F(S)$ to be the set of all words in S, where two such expressions are multiplied in $F(S)$ by concatenating them. Although in essence this is what we do, it is necessary to be more formal in order to prove that this concatenation operation is well defined and associative. After all, even the familiar notation a^n for the product $a \cdot a \cdots a$ (n terms) is permissible only because we know that this product is independent of the way it is bracketed (cf. the generalized associative law in Section 1.1). The formal construction of $F(S)$ is carried out below for an arbitrary set S.

One important property reflecting the fact that there are no relations that must be satisfied by the generators in S is that any *map* from the *set* S to a group G can be uniquely extended to a *homomorphism* from the *group* $F(S)$ to G (basically since we have specified where the generators must go and the images of all the other elements are uniquely determined by the homomorphism property — the fact that there are no relations to worry about means that we can specify the images of the generators *arbitrarily*). This is frequently referred to as the *universal* property of the free group and in fact characterizes the group $F(S)$.

The notion of "freeness" occurs in many algebraic systems and it may already be familiar (using a different terminology) from elementary vector space theory. When the algebraic systems are vector spaces, $F(S)$ is simply the vector space which has S as a basis. Every vector in this space is a unique linear combination of the elements of S (the analogue of a "word"). Any set map from the basis S to another vector space V extends uniquely to a linear transformation (i.e., vector space homomorphism) from $F(S)$ to V.

Before beginning the construction of $F(S)$ we mention that one often sees the universal property described in the language of commutative diagrams. In this form it reads (for groups) as follows: given any set map φ from the set S to a group G there is a unique homomorphism $\Phi : F(S) \to G$ such that $\Phi|_S = \varphi$ i.e., such that the following diagram commutes:



As mentioned above, the only difficulty with the construction of $F(S)$ is the verification that the concatenation operation on the words in $F(S)$ is well defined and associative. To prove the associative property for multiplication of words we return to the most basic level where all the exponents in the words of S are ± 1.

We first introduce inverses for elements of S and an identity.

Let S^{-1} be any set disjoint from S such that there is a bijection from S to S^{-1}. For each $s \in S$ denote its corresponding element in S^{-1} by s^{-1} and similarly for each $t \in S^{-1}$ let the corresponding element of S be denoted by t^{-1} (so $(s^{-1})^{-1} = s$). Take a singleton set not contained in $S \cup S^{-1}$ and call it $\{1\}$. Let $1^{-1} = 1$ and for any $x \in S \cup S^{-1} \cup \{1\}$ let $x^1 = x$.

Next we describe the elements of the free group on the set S. A *word* on S is by definition a sequence

$$(s_1, s_2, s_3, \dots) \quad \text{where } s_i \in S \cup S^{-1} \cup \{1\} \text{ and } s_i = 1 \text{ for all } i \text{ sufficiently large}$$

(that is, for each sequence there is an N such that $s_i = 1$ for all $i \geq N$). Thus we can think of a word as a finite product of elements of S and their inverses (where repetitions are allowed). Next, in order to assure uniqueness of expressions we consider only words which have no obvious "cancellations" between adjacent terms (such as $baa^{-1}b = bb$). The word $(s_1, s_2, s_3, \dots)$ is said to be *reduced* if

(1) $s_{i+1} \neq s_i^{-1}$ for all i with $s_i \neq 1$, and
(2) if $s_k = 1$ for some k, then $s_i = 1$ for all $i \geq k$.

The reduced word $(1, 1, 1, \dots)$ is called the *empty word* and is denoted by 1. We now simplify the notation by writing the reduced word $(s_1^{\epsilon_1}, s_2^{\epsilon_2}, \dots, s_n^{\epsilon_n}, 1, 1, 1, \dots)$, $s_i \in S$, $\epsilon_i = \pm 1$, as $s_1^{\epsilon_1} s_2^{\epsilon_2} \dots s_n^{\epsilon_n}$. Note that by definition, reduced words $r_1^{\delta_1} r_2^{\delta_2} \dots r_m^{\delta_m}$ and $s_1^{\epsilon_1} s_2^{\epsilon_2} \dots s_n^{\epsilon_n}$ are equal if and only if $n = m$ and $\delta_i = \epsilon_i$, $1 \leq i \leq n$. Let $F(S)$ be the set of reduced words on S and embed S into $F(S)$ by

$$s \mapsto (s, 1, 1, 1, \dots).$$

Under this set injection we identify S with its image and henceforth consider S as a subset of $F(S)$. Note that if $S = \emptyset$, $F(S) = \{1\}$.

We are now in a position to introduce the binary operation on $F(S)$. The principal technical difficulty is to ensure that the product of two reduced words is again a *reduced* word. Although the definition appears to be complicated it is simply the formal rule for "successive cancellation" of juxtaposed terms which are inverses of each other (e.g., $ab^{-1}a$ times $a^{-1}ba$ should reduce to aa). Let $r_1^{\delta_1} r_2^{\delta_2} \dots r_m^{\delta_m}$ and $s_1^{\epsilon_1} s_2^{\epsilon_2} \dots s_n^{\epsilon_n}$ be reduced words and assume first that $m \leq n$. Let k be the smallest integer in the range $1 \leq k \leq m+1$ such that $s_k^{\epsilon_k} \neq r_{m-k+1}^{-\delta_{m-k+1}}$. Then the product of these reduced words is defined to be:

$$(r_1^{\delta_1} r_2^{\delta_2} \dots r_m^{\delta_m})(s_1^{\epsilon_1} s_2^{\epsilon_2} \dots s_n^{\epsilon_n}) = \begin{cases} r_1^{\delta_1} \dots r_{m-k+1}^{\delta_{m-k+1}} s_k^{\epsilon_k} \dots s_n^{\epsilon_n}, & \text{if } k \leq m \\ s_{m+1}^{\epsilon_{m+1}} \dots s_n^{\epsilon_n}, & \text{if } k = m+1 \leq n \\ 1, & \text{if } k = m+1 \text{ and } m = n. \end{cases}$$

The product is defined similarly when $m \geq n$, so in either case it results in a reduced word.