(c) Given an angle θ, show that $e^{i\theta} = \cos\theta + i\sin\theta \in C$ and conversely, every element of $z \in C$ is of this form for a unique $\theta \in [0, 2\pi)$. This is another way to turn C into a group which is the *same* as the previous group in an appropriate sense.

We need to come back and check that $\mathbb{Z}_n$ is actually a group. We make use of a result usually called the "division algorithm". Although it's not an algorithm in the technical sense, it is the basis of the algorithm for long division that one learns in school.

Theorem 4.5. *Let x be an integer and n positive integer, then there exists a unique pair of integers q, r satisfying*

$$x = qn + r,\ 0 \leq r < n$$

Proof. Let

$$R = \{x - q'n \mid, q' \in \mathbb{Z} \text{ and } q'n \leq x\}$$

Observe that $R \subseteq \mathbb{N}$, so we can choose a smallest element $r = x - qn \in R$. Suppose $r \geq n$. Then $x = qn + r = (q+1)n + (r-n)$ means that $r - n$ lies in R. This is a contradiction, therefore $r < n$.

Suppose that $x = q'n + r'$ with $r' < n$. Then $r' \in R$ so $r' \geq r$. Then $qn = q'n + (r' - r)$ implies that $n(q - q') = r' - r$. So $r' - r$ is divisible by n. On the other hand $0 \leq r' - r < n$. But 0 is the only integer in this range divisible by n is 0. Therefore $r = r'$ and $qn = q'n$ which implies $q = q'$. $\square$

We denote the number r given above by $x \, mod \, n$, mod is read "modulo" or simply "mod". When $x \geq 0$, this is just the remainder after long divison by n.

Lemma 4.6. *If x_1, x_2, n are integers with $n > 0$, then*

$$(x_1 + x_2) \, mod \, n = (x_1 \, mod \, n) \oplus (x_2 \, mod \, n)$$

Proof. Set $r_i = x_i \, mod \, n$. Then $x_i = q_i n + r_i$ for appropriate q_i. We have $x_1 + x_2 = (q_1 + q_2)n + (r_1 + r_2)$. We see that

$$(x_1 + x_2) \, mod \, n = \begin{cases} r_1 + r_2 = r_1 \oplus r_2 & \text{if } r_1 + r_2 < n \\ r_1 + r_2 - n = r_1 \oplus r_2 & \text{otherwise} \end{cases}$$

$\square$

This would imply that $f(x) = x \, mod \, n$ gives a homomorphism from $\mathbb{Z} \to \mathbb{Z}_n$ if we already knew that $\mathbb{Z}_n$ were a group. Fortunately, this can be converted into a proof that it is one.

Lemma 4.7. *Suppose that $(G, *, e)$ is a group and $f : G \to H$ is an onto map to another set H with an operation $*$ such that $f(x * y) = f(x) * f(y)$. Then H is a group with identity $f(e)$.*

In the future, we usually just write $+$ for modular addition.

The dihedral group D_n is the full symmetry group of regular n-gon which includes both rotations and flips. There are $2n$ elements in total consisting

Chapter 5

Finite sets, counting and group theory

Let $\mathbb{N} = \{0, 1, 2 \ldots\}$ be the set of natural numbers. Given n, let $[n] = \{x \in \mathbb{N} \mid x < n\}$. So that $[0] = \emptyset$ is the empty set, and $[n] = \{0, 1, \ldots, n-1\}$ if $n > 0$. A set X is called *finite* if there is a one to one onto function (also called a one to one correspondence) $f : [n] \to X$ for some $n \in \mathbb{N}$. The choice of n is unique (which we will accept as a fact), and is called the cardinality of X, which we denote by $|X|$.

Lemma 5.1. *If X is finite and $g : X \to Y$ is a one to one correspondence, then Y is finite and $|Y| = |X|$.*

Proof. By definition, we have a one to one correspondence $f : [n] \to X$, where $n = |X|$. Therefore $g \circ f : [n] \to Y$ is a one to one correspondence. □

Proposition 5.2. *If a finite set X can be written as a union of two disjoint subsets $Y \cup Z$, then $|X| = |Y| + |Z|$. (Recall that $Y \cup Z = \{x \mid x \in Y \text{ or } x \in Z\}$, and disjoint means their intersection is empty.)*

Proof. Let $f : [n] \to Y$ and $g : [m] \to Z$ be one to one correspondences. Define $h : [n + m] \to X$ by

$$h(i) = \begin{cases} f(i) & \text{if } i < n \\ g(i - n) & \text{if } i \geq n \end{cases}$$

This is a one to one correspondence. □

A *partition* of X is a decomposition of X as a union of subsets $X = Y_1 \cup Y_2 \cup \ldots Y_n$ such that Y_i and Y_j are disjoint whenever $i \neq j$.

Corollary 5.3. *If $X = Y_1 \cup Y_2 \cup \ldots Y_n$ is a partition, then $|X| = |Y_1| + |Y_2| + \ldots |Y_n|$.*

Next, we want to develop a method for computing the order of a subgroup of S_n.

Definition 5.13. *Given $i \in \{1, \ldots, n\}$, the orbit $\mathrm{Orb}(i) = \{g(i) \mid g \in G\}$. A subgroup $G \subseteq S_n$ is called transitive if for some i, $\mathrm{Orb}(i) = \{1, \ldots, n\}$.*

Definition 5.14. *Given subgroup $G \subseteq S_n$ and $i \in \{1, \ldots n\}$, the stabilizer of i, is $\mathrm{Stab}(i) = \{f \in G \mid f(i) = i\}$*

Theorem 5.15 (Orbit-Stabilizer theorem)**.** *Given a subgroup $G \subseteq S_n$, and $i \in \{1, \ldots, n\}$ then*

$$|G| = |\mathrm{Orb}(i)| \cdot |\mathrm{Stab}(i)|$$

In particular,

$$|G| = n|\mathrm{Stab}(i)|$$

if G is transitive.

Proof. We define a function $f : G \to \mathrm{Orb}(i)$ by $f(g) = g(i)$. The preimage $T = f^{-1}(j) = \{g \in G \mid g(i) = j\}$. By definition if $j \in \mathrm{Orb}(i)$, there exists $g_0 \in T$. We want to show that $T = g_0 \mathrm{Stab}(i)$. In one direction, if $h \in \mathrm{Stab}(i)$ then $g_0 h(i) = j$. Therefore $g_0 h \in T$. Suppose $g \in T$. Then $g = g_0 h$ where $h = g_0^{-1} g$. We see that $h(i) = g_0^{-1} g(i) = g_0^{-1}(j) = i$. Therefore, we have established that $T = g_0 \mathrm{Stab}(i)$. This shows that

$$|G| = \sum_{j \in \mathrm{Orb}(i)} |f^{-1}(j)| = \sum_{j \in \mathrm{Orb}(i)} |\mathrm{Stab}(i)| = |\mathrm{Orb}(i)| \cdot |\mathrm{Stab}(i)|$$

∎

Corollary 5.16. $|S_n| = n!$

Proof. We prove this by mathematical induction starting from $n = 1$. When $n = 1$, S_n consists of the identity so $|S_1| = 1 = 1!$. In general, assuming that the corollary holds for n, we have prove it for $n+1$. The group S_{n+1} acts transitively on $\{1, \ldots, n+1\}$. We want to show that there is a one to one correspondence between $\mathrm{Stab}(n+1)$ and S_n. An element of $f \in \mathrm{Stab}(n+1)$ looks like

$$\begin{pmatrix} 1 & 2 & \ldots n & n+1 \\ f(1) & f(2) & \ldots f(n) & n+1 \end{pmatrix}$$

Dropping the last column yields a permutation in S_n, and any permutation in S_n extends uniquely to an element of $\mathrm{Stab}(n+1)$ by adding that column. Therefore we have established the correspondence. It follows that $|\mathrm{Stab}(n+1)| = |S_n| = n!$. Therefore

$$|S_{n+1}| = (n+1)|\mathrm{Stab}(n+1)| = (n+1)(n!) = (n+1)!$$

∎

Proposition 7.10. *$SO(2)$ is a normal subgroup of $O(2)$.*

We give two proofs. The first, which uses determinants, gets to the point quickly. However, the second proof is also useful since it leads to the formula (7.1).

First Proof. We start with a standard result.

Theorem 7.11. *For any pair of 2×2 matrices A and B, $\det AB = \det A \det B$.*

Proof. A brute force calculation shows that

$$(a_{11}a_{22} - a_{12}a_{21})(b_{11}b_{22} - b_{12}b_{21})$$

and

$$(a_{11}b_{11} + a_{12}b_{21})(a_{21}b_{12} + a_{22}b_{22}) - (a_{11}b_{12} + a_{12}b_{22})(a_{21}b_{11} + a_{22}b_{22})$$

both can be expanded to

$$a_{11}a_{22}b_{11}b_{22} - a_{11}a_{22}b_{12}b_{21} - a_{12}a_{21}b_{11}b_{22} + a_{12}a_{21}b_{12}b_{21}$$

$\square$

Therefore $\det : O(2) \to \mathbb{R}^*$ is a homomorphism, where $\mathbb{R}^*$ denote the group of nonzero real numbers under multiplication. It follows that $SO(2)$ is the kernel. So it is normal. $\square$

Second Proof. We have to show that $AR(\theta)A^{-1} \in SO(2)$ for any $A \in O(2)$. This is true when $A \in SO(2)$ because $SO(2)$ is a subgroup.

It remains to show that conjugating a rotation by a reflection is a rotation. In fact we will show that for any reflection A

$$AR(\theta)A^{-1} = R(-\theta) \tag{7.1}$$

First let A be the reflection $F = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ about the x-axis. Then an easy calculation shows that $FR(\theta)F^{-1} = FR(\theta)F = R(-\theta)$. Now assume that A is a general reflection. Then

$$A = \begin{bmatrix} \cos\phi & \sin\phi \\ \sin\phi & -\cos\phi \end{bmatrix} = FR(-\phi)$$

So

$$AR(\theta)A^{-1} = FR(-\phi)R(\theta)R(\phi)F = R(-\theta)$$

as claimed. $\square$

So now we have a normal subgroup $SO(2) \subset O(2)$ which we understand pretty well. What about the quotient $O(2)/SO(2)$. This can identified with the cyclic group $\{\pm 1\} \subset \mathbb{R}^*$ using the determinant.

Chapter 9

$\mathbb{Z}_p^*$ is cyclic

Given a field K, a polynomial in x is a symbolic expression

$$a_n x^n + a_{n_1} x^{n-1} + \ldots + a_0$$

where $n \in \mathbb{N}$ is arbitrary and the coefficients $a_n, \ldots, a_0 \in K$. Note that polynomials are often viewed as functions but it is important to really treat these as expressions. First of all the algebraic properties become clearer, and secondly when K is finte, there only finitely many functions from $K \to K$ but infinitely many polynomials. We denote the set of these polynomials by $K[x]$. We omit terms if the coefficients are zero, so we can pad out a polynomial with extra zeros whenever convenient e.g. $1 = 0x^2 + 0x + 1$. The highest power of x occurring with a nonzero coefficient is called the degree. We can add polynomials by adding the coefficients

$$f = a_n x^n + a_{n_1} x^{n-1} + \ldots + a_0$$

$$g = b_n x^n + b_{n_1} x^{n-1} + \ldots + b_0$$

$$f + g = (a_n + b_n) x^n + \ldots (a_0 + b_0)$$

Multiplication is defined using the rules one learns in school

$$\begin{aligned} fg &= (a_0 b_0) + (a_1 b_0 + a_0 b_1) x + (a_2 b_0 + a_1 b_1 + a_0 b_2) x^2 + \ldots \\ &= (\sum_{i+j=k} a_i b_j) x^k \end{aligned}$$

Theorem 9.1. *$K[x]$ is a commutative ring with the operations described above.*

Proof. This is fairly routine, so we just list a few steps. Let f and g be as above and

$$h = c_n x^n + c_{n-1} x^{n-1} + \ldots c_0$$

Then

$$f(gh) = (\sum_{i+j+k=\ell} a_i b_j c_k) x^\ell = (fg)h$$

We now apply these results to the field $K = \mathbb{Z}_p$, where p is a prime. Sometimes this is denoted by $\mathbb{F}_p$ to emphasize that its a field. When the need arises, let us write $\overline{a}$ to indicate we are working $\mathbb{Z}_p$, but we won't bother when the context is clear.

Proposition 9.5. *We can factor $x^p - x = x(x-1)(x-2)\ldots(x-(p-1))$ in $\mathbb{Z}_p[x]$*

Proof. By Fermat's little theorem, $1\ldots,p-1$ are roots. Therefore $x^p - x = x(x-1)(x-2)\ldots(x-p-1)$ in $\mathbb{Z}_p[x]$. □

Corollary 9.6 (Wilson's theorem)**.** $\overline{(p-1)!} = -\overline{1}$

Proof. We have $x^{p-1} - 1 = (x-1)(x-2)\ldots(x-(p-1))$. Now evaluate both sides at 0. □

Corollary 9.7. *The binomial coefficients $\binom{p}{n} = \frac{p!}{n!(p-n)!}$ are divisible by n when $1 < n < p$.*

Proof. Substitue $1+x$ into the above identity to obtain $(1+x)^p - (1+x) = 0$ in $\mathbb{Z}_p$. Now expand using the binomial theorem, which is valid in any field (see exercises), to obtain

$$\sum_{n=1}^{p-1} \overline{\binom{p}{n}} x^n = 0$$

□

The last few results were fairly easy, the next result is not.

Theorem 9.8. *If p is prime, then $\mathbb{Z}_p^*$ is cyclic.*

Proof in a special case. We won't prove this in general, but to get some sense of why this is true, let's prove it when $p = 2q+1$, where q is another prime. This is not typical, but it can certainly happen (e.g. $p = 7, 11, 23, \ldots$). Then $\mathbb{Z}_p^*$ has order $2q$. The possible orders of its elements are $1, 2, q$, or $2q$. There is only element of order 1, namely 1. An element of order 2 is a root of $x^2 - 1$, so it must be $-\overline{1}$. An element of order q satisfies $x^q - 1 = 0$, and be different from 1. Thus there are at most $q-1$ possibilities. So to summarize there are no more $q+1$ elements of orders $1, 2, q$. Therefore there are at least $q-1$ elements of order $2q$, and these are necessarily generators. □

9.9 Exercises

1. Given a field K and a positive integer n, let $\overline{n} = 1 + \ldots + 1$ (n times). K is said to have *positive characteristic* if $\overline{n} = 0$ for some positive n, otherwise K is said to have characteristic 0. In the positive characteristic case, the smallest $n > 0$ with $\overline{n} = 0$ is called the *characteristic*. Prove that the characteristic is a prime number.

2. For any field, prove the binomial theorem

$$(x+1)^n = \sum_{m=0}^{n} \binom{n}{m} x^m$$

(Recall $\binom{n+1}{m} = \binom{n}{m} + \binom{n+1}{m}$.)

3. Let K be a field and $s \in K$. Let $K[\sqrt{s}]$ be the set of expressions $a + b\sqrt{s}$, with $a, b \in K$. Show that this becomes a commutative ring if we define addition and multiplication as the notation suggests:

$$(a + bi\sqrt{s}) + (c + d\sqrt{s}) = (a + c) + (b + d)\sqrt{s}$$

$$(a + b\sqrt{s})(c + d\sqrt{s}) = (ac + bds) + (ad + bc)\sqrt{s}$$

4. Show $K[\sqrt{s}]$ has zero divisors if $x^2 - s = 0$ has a root. If this equation does not have a root, then prove that $K[\sqrt{s}]$ is a field (Hint: $(a+b\sqrt{s})(a-b\sqrt{s}) =?$ and when is it zero?).

5. When p is an odd prime, show that the map $x \mapsto x^2$ from $\mathbb{Z}_p \to \mathbb{Z}_p$ is not onto. Use this fact to construct a field with p^2 elements and characteristic p.

Chapter 12

Determinants

The ideas of the previous chapter can be applied to linear algebra. Given an $n \times n$ matrix $A = [a_{ij}]$ over a field K, the *determinant*

$$\det A = \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) a_{1\sigma(1)} \dots a_{n\sigma(n)}$$

This is bit like the antisymmetrization considered earlier. There is also symmetric version, without $\operatorname{sign}(\sigma)$, called the permanent. However, as far as I know, it is much less useful. The definition, we gave for the determinant, is not very practical. However, it is theoretically quite useful.

Theorem 12.1. *Given an $n \times n$ matrix A, the following properties hold.*

(a) $\det I = 1$

(b) If B is obtained by multiplying the ith row of A by b then $\det B = b \det A$

(c) Suppose that the ith row of C is the sum of the ith rows of A an B, and all other rows of A, B and C are identical. Then $\det C = \det A + \det B$.

(d) $\det A = \det A^T$.

(e) Let us write $A = [v_1, \dots, v_n]$, where $v_1, v_2, \dots$ are the columns. Then $\det(v_{\tau(1)}, \dots v_{\tau(n)}) = \operatorname{sign}(\tau) \det(v_1, \dots v_n)$

Proof. Item (a) is clear because all the terms $\delta_{1\sigma(1)} \dots \delta_{n\sigma(n)} = 0$ unless $\sigma = I$.
(b)

$$\begin{aligned} \det B &= \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) a_{1\sigma(1)} \dots (b a_{i\sigma(i)}) \dots a_{n\sigma(n)} \\ &= b \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) a_{1\sigma(1)} \dots a_{i\sigma(i)} \dots a_{n\sigma(n)} \\ &= b \det A \end{aligned}$$

Proof. The characteristic polynomial $p(\lambda) = \lambda^3 + a_2\lambda^2 + \ldots$ has real coefficients. Since λ^3 grows faster than the other terms, $p(\lambda) > 0$ when $\lambda \gg 0$, and $p(\lambda) < 0$ when $\lambda \ll 0$. Therefore the graph of $y = p(x)$ must cross the x-axis somewhere, and this would give a real root of p. (This intuitive argument is justified by the intermediate value theorem from analysis.)

$\square$

Lemma 13.5. *If $A \in O(3)$, 1 or -1 is an eigenvalue.*

Proof. By the previous lemma, there exists a nonzero vector $v = [x, y, z]^T \in \mathbb{R}^3$ and real number λ such that $Av = \lambda v$. Since a multiple of v will satisfy the same conditions, we can assume that the square of the length $v^T v = x^2 + y^2 + z^2 = 1$. It follows that

$$\lambda^2 = (\lambda v)^T(\lambda v) = (Av)^T(Av) = v^T A^T A v = v^T v = 1$$

$\square$

Theorem 13.6. *A matrix in $SO(3)$ is a rotation.*

Proof. Let $R \in SO(3)$. By the previous lemma, ± 1 is an eigenvalue.

We divide the proof into two cases. First suppose that 1 is eigenvalue. Let v_3 be an eigenvector with eigenvalue 1. We can assume that v_3 is a unit vector. We can complete this to an orthonormal set v_1, v_2, v_3. The vectors v_1 and v_2 form a basis for the plane $v_3^\perp$ perpendicular to v_3. The matrix $A = [v_1, v_2, v_3]$ is orthogonal, and we can assume that it is in $SO(3)$ by switching v_1 and v_2 if necessary. It follows that

$$RA = [Rv_1, Rv_2, Rv_3] = [Rv_1, Rv_2, v_3]$$

remains orthogonal. Therefore Rv_1, Rv_2 lie in $v_3^\perp$. Thus we can write

$$\begin{aligned} R(v_1) &= av_1 + bv_2 \\ R(v_2) &= cv_1 + dv_2 \\ R(v_3) &= v_3 \end{aligned}$$

The matrix

$$A^{-1}RA = \begin{bmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

lies in $SO(3)$. It follows that the block $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ lies in $SO(2)$, which means that it is a plane rotation matrix $R(\theta)$. It follows that $R = R(\theta, v_3)$.

Now suppose that -1 is an eigenvalue and let v_3 be an eigenvector. Defining A as above, we can see that

$$A^{-1}RA = \begin{bmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & -1 \end{bmatrix}$$

This time the upper 2×2 is block lies $O(2)$ with determinant -1. This implies that it is a reflection. This means that there is a nonzero vector v in the plane $v_3^\perp$ such $Rv = v$. Therefore R also $+1$ as an eigenvalue, and we have already shown that R is a rotation. $\square$

From the proof, we extract the following useful fact.

Corollary 13.7. *Every matrix in $SO(3)$ has $+1$ as an eigenvalue. If the matrix is not the identity then the corresponding eigenvector is the axis of rotation.*

We excluded the identity above, because everything would be an axis of rotation for it. Let us summarize everything we've proved in one statement.

Theorem 13.8. *The set of rotations in $\mathbb{R}^3$ can be identified with $SO(3)$, and this forms a group.*

13.9 Exercises

1. Check that unlike $SO(2)$, $SO(3)$ is not abelian. (This could get messy so choose the matrices with care.)

2. Given two rotations $R_i = R(\theta_i, v_i)$, show that the axis of $R_2 R_1 R_2^{-1}$ is $R_2 v_1$. Conclude that a normal subgroup of $SO(3)$, different from $\{I\}$, is infinite.

3. Check that
$$\begin{bmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{bmatrix}$$
has $1, e^{\pm i\theta}$ as complex eigenvalues. With the help of the previous exercise show that this holds for any rotation $R(\theta, v)$.

4. Show the map $f : O(2) \to SO(3)$ defined by
$$f(A) = \begin{bmatrix} A & 0 \\ 0 & \det(A) \end{bmatrix}$$
is a one to one homomorphism. Therefore we can view $O(2)$ as a subgroup of $SO(3)$. Show that this subgroup is the subgroup $\{g \in SO(3) \mid gr = \pm r\}$, where $r = [0, 0, 1]^T$.

5. Two subgroups $H_i \subseteq G$ of a group are *conjugate* if for some $g \in G$, $H_2 = gH_1g^{-1} := \{ghg^{-1} \mid h \in H_1\}$. Prove that $H_1 \cong H_2$ if they are conjugate. Is the converse true?

6. Prove that for any nonzero vector $v \in \mathbb{R}^3$, the subgroup $\{g \in SO(3) \mid gv = \pm v\}$ (respectively $\{g \in SO(3) \mid gv = v\}$) is conjugate, and therefore isomorphic, to $O(2)$ (respectively $SO(2)$). (Hint: use the previous exercises.)

Lemma 14.5. *If $n = 2$, G is cyclic.*

Proof. Since $\mathrm{Stab}(p_i) \subseteq G$, we have

$$\left(1 - \frac{1}{|\mathrm{Stab}(p_i)|}\right) \leq \left(1 - \frac{1}{|G|}\right) \tag{14.2}$$

But (14.1) implies

$$2\left(1 - \frac{1}{|G|}\right) = \left(1 - \frac{1}{|\mathrm{Stab}(p_1)|}\right) + \left(1 - \frac{1}{|\mathrm{Stab}(p_2|}\right)$$

and this forces equality in (14.2) for both $i = 1, 2$. This implies that $G = \mathrm{Stab}(p_1) = \mathrm{Stab}(p_2)$. This means that $g \in G$ is a rotation with axis the line L connecting p_1 to 0 (or p_2 to 0, which would have to be the same). It follows that g would have to be a rotation in the plane perpendicular to L. So that G can be viewed as subgroup of $SO(2)$. Therefore it is cyclic by theorem 14.1. $\square$

We now turn to the case $n = 3$. Let us set $n_i = |\mathrm{Stab}(p_i)|$ and arrange them in order $2 \leq n_1 \leq n_2 \leq n_3$. (14.1) becomes

$$2\left(1 - \frac{1}{|G|}\right) = \left(1 - \frac{1}{n_1}\right) + \left(1 - \frac{1}{n_2}\right) + \left(1 - \frac{1}{n_3}\right)$$

or

$$1 + \frac{2}{|G|} = \frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3}$$

The left side is greater than one, so we have a natural constraint.

Lemma 14.6. *The only integer solutions to the inequalities*

$$2 \leq n_1 \leq n_2 \leq n_3$$

$$\frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3} > 1$$

are as listed together with the corresponding orders of G.

(a) $(2, 2, n_3)$ *and* $|G| = 2n_3$.

(b) $(2, 3, 3)$ *and* $|G| = 12$.

(c) $(2, 3, 4)$ *and* $|G| = 24$.

(d) $(2, 3, 5)$ *and* $|G| = 60$.

To complete the proof of theorem 14.2, we need the following

Lemma 14.7. *A subgroup $G \subset SO(3)$ corresponding to the triple $(2, 2, n)$ is isomorphic to D_n.*