1. How many rotationally distinct ways are there to 3-color the faces of a dodecahedron?

Answer: In 9099 ways.

This is an application of the Burnside counting theorem. Let $G \cong A_5$ be the symmetry group of the dodecahedron. Let $S$ be the set of 3-colorings of a dodecahedron with labeled faces. The answer to the question is given by the number of orbits for the natural action of $G$ on this set $S$. The group $G \cong A_5$ has five conjugacy classes of respective sizes 1, 12, 12, 15, 30: these are (1) the identity; (2) the $2\pi/5$-rotations about a line joining the centers of a pair of opposite faces; (3) $4\pi/5$-rotations about a line joining the centers of a pair of opposite faces; (4) $\pi$-degree rotations about a line joining the midpoints of two antipodal edges; and (5) $2\pi/3$-rotation about a line joining a pair of antipodal vertices. The stabilizers in $G$ for these conjugacy classes have respective sizes $3^{12}, 3^{4}, 3^{4}, 3^{6}, 3^{4}$. By Burnside’s counting theorem (Theorem 10.12 in the Course Notes), the number of orbits for the action is equal to

$$|S/G| = \frac{1}{60}(1 \cdot 3^{12} + 12 \cdot 3^{4} + 12 \cdot 3^{4} + 15 \cdot 3^{6} + 20 \cdot 3^{4}) = 9099,$$

which is the answer to the question.

---

2. Prove that if $p$ is prime, then $(\mathbb{Z}/p)^*$ is cyclic.

By the Euclidean division algorithm, a polynomial of degree $d$ has at most $d$ zeros over any field. Applying this to the polynomial $x^d - 1$ over the finite field $\mathbb{F}_p = \mathbb{Z}/p$, we conclude that, for every $d > 0$, the group $(\mathbb{Z}/p)^*$ has at most $d$ elements of order dividing $d$. In other words, the finite abelian group $(\mathbb{Z}/p)^*$ has at most one subgroup of any given order. It follows from the structure theorem of finite abelian groups that a group with this property is necessarily cyclic: a finite abelian group is isomorphic to $\mathbb{Z}/d_1 \times \cdots \times \mathbb{Z}/d_r$ for its invariant factors $d_1 \mid d_2 \mid \cdots \mid d_r$, and would have two distinct subgroups of order $d_1$ if $r > 1$; hence $r = 1$, and the group is cyclic. Consequently: the group $\mathbb{F}_p^*$ of units of the finite field $\mathbb{F}_p$ is cyclic of order $p - 1$. 

---

1
Remark. In the elementary theory of numbers, this result is referred to as the existence of a primitive element mod $p$. The proof shows, more generally, that the group of units of any finite field is cyclic. One application of this result is that the group $\text{GL}_2(\mathbb{F}_p)$ contains an element of order $p^2 - 1$: one may construct a field $F$ with $p^2$ elements, whose group $F^\times$ of units must be cyclic of order $p^2 - 1$ by the above argument; let $\alpha \in F^\times$ be a generator. Then $F$ can be considered as a two-dimensional $\mathbb{F}_p$-vector space, and the $\mathbb{F}_p$-automorphism $F \to F, x \mapsto \alpha x$ becomes an invertible linear transformation of order $p^2 - 1$.

3. Prove that if $n = pq$ is a product of primes satisfying $p \mid q - 1$, then there is a unique nonabelian group of order $n$ up to isomorphism.

A nonabelian group of order $pq$ is constructed as a semidirect product of the cyclic groups $\mathbb{Z}/q$ and $\mathbb{Z}/p$ relative to any nontrivial homomorphism $\mathbb{Z}/p \to \text{Aut}(\mathbb{Z}/q) = (\mathbb{Z}/q)^* \cong \mathbb{Z}/(q-1)$ (which exists, since $p \mid q - 1$ implies that $\text{Aut}(\mathbb{Z}/q) \cong \mathbb{Z}/(q-1)$ has an element of order $p$).

Suppose $G$ is any nonabelian group of order $pq$. For at least two reasons, $G$ must have a normal subgroup of order $q$. The first reason are the Sylow theorems, which give that the number of order-$q$ subgroups of $G$ divides $p$ and is $\equiv 1 \mod q$; as $q > p$ and $p$ is prime, this number is 1, and the unique $q$-Sylow subgroup $H$ of $G$ is normal. The second reason is that, in an arbitrary finite group $G$, all subgroups of index the minimal prime dividing $|G|$ are normal.

From Problem 2 above, the group $\text{Aut} H \cong \mathbb{Z}/(q-1)$ is cyclic of order $q - 1$, and hence has a unique subgroup of order $p$; fix a generator $\sigma$ for this group (that is, $\sigma$ is a choice of an element of order $p$). Let $A$ be a $p$-Sylow subgroup of $G$ (that is, a subgroup of order $p$). Then $A, H$ have complementary orders and intersect trivially; it follows that they are complementary subgroups, and since $H$ is normal, it follows by Theorem 10.13 from the Course Notes that $G = H \rtimes A$ is a semidirect product for the action of $A$ on $H$ by conjugation. The latter action is nontrivial since $G$ is nonabelian, and determines a nontrivial homomorphism $A \to \text{Aut} H$, whose is therefore injective with image the unique order-$p$ subgroup $\langle \sigma \rangle$ of $\text{Aut} H$. There is a unique isomorphism $\mathbb{Z}/p \cong A$ whose composition with $A \to \text{Aut} H$ maps $1 + p\mathbb{Z}$ to $\sigma$, and this completely determines the composition $\mathbb{Z}/p \to \text{Aut} H$. Thus $G$ is isomorphic to the semidirect product constructed in the opening paragraph.

Remark. At this point, we have a complete classification of groups of
order composed of at most two prime factors. For order $p^2$, there are two groups, both abelian. For order $pq$ with $p \nmid q - 1$, there is a unique group, the cyclic group of that order. For order $pq$ with $p \mid q - 1$, there are exactly two groups, one cyclic and one nonabelian. This simple classification can extended to order $pqr$, where the groups are still described by the simple arithmetic conditions of Sylow theory; but it breaks down for four or more prime factors: $A_5$, for example, is a simple group of order $60 = 2^3 \cdot 3 \cdot 5$.

4. Prove that $\mathbb{Z}/a \times \mathbb{Z}/b$ is isomorphic to $\mathbb{Z}/c \times \mathbb{Z}/(ab/c)$, where $c = \gcd(a, b)$.

Using this, prove any product of finite cyclic groups is isomorphic to a unique product of the form $\mathbb{Z}/a_1 \times \cdots \times \mathbb{Z}/a_n$, where $a_1 \mid a_2 \mid \cdots \mid a_n$.

The special case with $\gcd(a, b) = 1$ is called the Chinese remainder theorem: the map $\mathbb{Z}/(ab) \to \mathbb{Z}/a \times \mathbb{Z}/b, \quad x \mapsto (x \mod a, x \mod b)$ is an isomorphism. This follows from the pigeonhole principle upon verifying injectivity, which is immediate: when $\gcd(a, b) = 1$, $a \mid x$ and $b \mid x$ imply $ab \mid x$. For the general case, write $c = ra - bs$ with $r, s \in \mathbb{Z}$, and define similarly the map $\mathbb{Z}/c \times \mathbb{Z}/(ab/c) \to \mathbb{Z}/a \times \mathbb{Z}/b, \quad (y, x) \mapsto \left(\frac{ra}{c}y + x \mod a, \frac{ab}{c}y + x \mod b\right)$. This map is a well-defined homomorphism as $y \mod c$ determines $\frac{a}{c}y \mod a$ and $\frac{b}{c}y \mod b$, and it is sufficient, by the pigeonhole principle, to verify its injectivity: $a \mid \frac{ra}{c}y + x$ and $b \mid \frac{ab}{c}y + x$ imply $c \mid y, \frac{ab}{c} \mid x$. Since $c \mid a$ and $c \mid b$, it is clear that $\frac{c}{a}y + x) - \left(\frac{ra}{c}y + x\right) = ra-bsy = y$, as required. It then follows that $a \mid x$ and $b \mid x$, which implies that the least common multiple $\frac{ab}{c} \mid x$. Hence our map $\mathbb{Z}/c \times \mathbb{Z}/(ab/c) \to \mathbb{Z}/a \times \mathbb{Z}/b$ is an isomorphism.

It then follows by an easy induction that every product of finite cyclic groups $\mathbb{Z}/b_1 \times \cdots \times \mathbb{Z}/b_n$ is isomorphic to a product of the form $\mathbb{Z}/a_1 \times \cdots \times \mathbb{Z}/a_n$ with $a_1 \mid \cdots \mid a_n$. In detail, apply induction on the number of pairs $\{b_i, b_j\}$ with neither $b_i \mid b_j$ nor $b_j \mid b_i$. The induction is vacuous; for the induction step, consider such a pair $\{i, j\}$; then $G = \mathbb{Z}/b_i \times \mathbb{Z}/b_j \times A$, where $A$ is a group for which the induction hypothesis applies. By the first part, $\mathbb{Z}/b_i \times \mathbb{Z}/b_j \cong \mathbb{Z}/c \times \mathbb{Z}/m$, where $c := \gcd(b_i, b_j), m := \text{lcm}(b_i, b_j)$. Then $G \cong \mathbb{Z}/c \times \mathbb{Z}/m \times A$; and it suffices to justify that the right-hand side satisfies the induction hypothesis. In what follows, $k \in \{1, \ldots, r\}$ denotes an index not in $\{i, j\}$. A pair $\{c, b_k\}$ with $c \nmid b_k$ and $b_k \nmid c$ induces either the pair $\{b_k, b_j\}$ with $b_k \nmid b_j$ or the pair $\{b_j, b_k\}$ with $b_j \nmid b_k$. A pair $\{m, b_k\}$ with $b_k \nmid m$ induces either the pair $\{b_i, b_k\}$ with $b_k \nmid b_i$ or the pair $\{b_j, b_k\}$ with $b_k \nmid b_j$. Since the pair $\{b_i, b_j\}$ has been replaced by the pair $\{c, m\}$ satisfying $c \mid m$, it follows from the induction hypothesis.
that $G \cong \mathbb{Z}/c \times \mathbb{Z}/m \times A$ is of the required form.

5. Prove that the statement every abelian group of order $n$ is cyclic holds if and only if $n$ is the product of distinct primes.

That $n$ must be square-free follows from the existence of the noncyclic abelian group $\mathbb{Z}/p \times \mathbb{Z}/p$ of order $p^2$. Conversely, if $n$ is square-free and $G \cong \mathbb{Z}/d_1 \times \cdots \times \mathbb{Z}/d_r$ an abelian group of order $n$ written in invariant form with $1 < d_1 | \cdots | d_r$, then $n = d_1 \cdots d_r$ forces $r = 1$: else, $n$ would be divisible by $d_1^2$ and would not be square-free.

6. For which values of $n$ is $D_n$ nilpotent?

**Answer:** The dihedral group $D_n$ of order $2n$ is nilpotent if and only if $n$ is a power of 2. If $n$ is a power of 2, then $D_n$ is a 2-group, in particular nilpotent. If $n$ is odd, then $D_n$ has trivial center and hence can not be nilpotent. Finally, if $n$ is even and $r \in D_n$ is a rotation of order $n$, then the center $Z(D_n)$ is the group $\{1, r^{n/2}\}$, and the quotient group $D_n/Z(D_n)$ is isomorphic to $D_{n/2}$; the assertion follows.

7. Let $N \subset \text{GL}_n(\mathbb{R})$ be the group of upper-triangular matrices with 1’s along the diagonal. Prove that $N$ is a nilpotent group (i) for $n = 3$; (ii) for $n = 4$.

(i) The first step is to find the center of $N$; as shows an immediate calculation, it consists of the matrices of the form

$$
\begin{pmatrix}
1 & * \\
1 & 1 \\
1 & 1
\end{pmatrix},
$$

with the only possible nonzero off-diagonal entry in the upper-right corner. The quotient $N/Z(N)$ is isomorphic to $\mathbb{Z}^2$, which is abelian; thus, $N$ is nilpotent.

(ii) Similarly, the center of $N$ is isomorphic to $\mathbb{Z}$, consisting of the matrices

$$
\begin{pmatrix}
1 & * \\
1 & 1 \\
1 & 1
\end{pmatrix}.
$$
The center of the quotient group \( N_1 := N/Z(N) \) consists of classes of matrices containing a representative of the form

\[
\begin{pmatrix}
1 & * \\
1 & 1 \\
1 & 1
\end{pmatrix}.
\]

The quotient \( N_1/Z(N_1) \) is then isomorphic to \( \mathbb{Z}^3 \), which is abelian; consequently, \( N_1 \), and hence \( N \), is nilpotent.

8. Find all the groups of order 8, up to isomorphism.

There are five groups of order 8 (just as there are five groups of any cube-of-prime order \( p^3 \)), three of which are abelian (those are \( \mathbb{Z}/8, \mathbb{Z}/4 \times \mathbb{Z}/2, \) and \( \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \)), and two nonabelian (the dihedral group \( D_4 \) and the group of quaternions \( Q \)). To show that these exhaust all possibilities, consider an arbitrary nonabelian group \( G \) of order 8. Then \( G \) must have an element of order 4: else, all elements would be of order 1 or 2, and a group with this property is abelian. Letting \( x \in G \) for an element of order 4, note that the cyclic subgroup \( \langle x \rangle \) has index 2 and is hence normal. Take any \( y \in G - \langle x \rangle \); then \( \langle x, y \rangle = G \), since an index-2 subgroup is always maximal. Then \( [x, y] \neq 1 \), because \( G \) is nonabelian. Thus \( yxy^{-1} \in \langle x \rangle = \{1, x, x^2, x^{-1}\} \), which has order 4, cannot equal \( x \) and must therefore equal \( x^{-1} \): \( yxy^{-1} = x^{-1} \). On the other hand, since \( y^2 \in \langle x \rangle \) has order 1 or 2, there are two possibilities: either \( y^2 = 1 \), or \( y^2 = x^2 \). We obtain that either

\[
G = \langle x, y \mid x^4 = y^2 = 1, yxy^{-1} = x^{-1} \rangle,
\]

and \( G \) is isomorphic to the symmetry group \( D_4 \) of the square by sending \( x \) to a rotation and \( y \) to a reflection; or

\[
G = \langle x, y \mid x^4 = 1, y^2 = x^2, yx = x^2 \cdot (xy) \rangle,
\]

which is isomorphic to the quaternion group via \( x \mapsto i, y \mapsto j, xy \mapsto k \).

9. Let \( N \subset \text{GL}_3(\mathbb{F}_2) \) be the group of invertible upper-triangular matrices. Is \( N \) isomorphic to \( D_4 \) or to the quaternion group \( Q \)?
Since $N$ is a nonabelian group of order $8$, it must be isomorphic to either $D_4$ or $Q$. Since it contains the two different elements

\[
\begin{pmatrix}
1 & 1 & 0 \\
0 & 1 & 0 \\
0 & 0 & 1
\end{pmatrix}, \quad \begin{pmatrix}
1 & 0 & 0 \\
0 & 1 & 1 \\
0 & 0 & 1
\end{pmatrix}
\]

of order 2, it cannot be isomorphic to $Q$ (which has $-1$ as its unique order-2 element). Therefore, $N$ is isomorphic to $D_4$.

10. (i) Show that the group of affine symmetries $g(x) = Ax + b$ of the finite plane $F_2^2$ is isomorphic to $S_4$. (ii) Show that $S_4$ is the semidirect product of a subgroup of order 4 and a subgroup of order 6.

(i) The finite plane $F_2^2$ has four elements, $e := (0,0), p := (0,1), q := (1,0), r := (1,1)$. Let $G$ be the its group of affine symmetries. The action of $G$ on $F_2^2$ determines a homomorphism $\phi : G \to S_4$ that we wish to show is an isomorphism; for this it suffices to show that $\phi$ is injective and $|G| = 24$. Injectivity means that $Ax + b = x$ identically on $x \in F_2^2$ implies $A = I$ and $b = 0$; this yields first of all $b = 0$, and the condition then rewrites $(A - I)x = 0$ for all $x \in F_2^2$, clearly yielding $A - I = 0$. It remains to show $|G| = 24$, which follows from the semidirect product decomposition $G \cong \text{GL}_2(F_2) \ltimes F_2^2$ analogous to the semidirect product decomposition $\text{Isom}(\mathbb{R}^2) \cong O_2(\mathbb{R}) \ltimes \mathbb{R}^2$: since $|\text{GL}_2(F_2)| = (2^2 - 1) \cdot (2^2 - 2) = 6$, this semidirect product implies $|G| = 6 \cdot 4 = 24$, as required.

(ii) It follows from part (i) that $S_4 \cong \text{GL}_2(F_2) \ltimes F_2^2$ is a semidirect product of a normal subgroup of order 4 and a subgroup of order 6.