

1. Give the definitions of the following terms:

(a) Sylow p -subgroup: Let G be a finite group, and let p be a prime number such that p divides the order of G . A *Sylow p -subgroup* of G is a subgroup H of G such that the order of H is p^k , where p^k is the largest power of p that divides the order of G .

(b) Galois group: Let K be a field extension of F . The *Galois group* of K over F , denoted $G(K/F)$, is the group of all field isomorphisms $\phi : K \rightarrow K$ such that $\phi(a) = a$ for all $a \in F$.

(c) Galois extension: Let K be a field extension of F . The field K is a *Galois extension* of F if the degree $[K : F]$ is finite and $|G(K/F)| = [K : F]$.

2. Find the number of different circular bracelets that can be made with 3 red beads, 2 white beads, and 1 blue bead. Show your reasoning.

The total number of beads is $3 + 2 + 1 = 6$. Since they are arranged in a circle, we can arrange the beads at the vertices of a regular hexagon with symmetry group $G = D_6$, and $|G| = 12$.

The set S of positions of the beads has 60 elements, since there are $\binom{6}{3} = 20$ choices for the positions of the three red beads, and then 3 remaining choices for the position of the blue bead.

The group G acts on the set S , and to apply Burnside's formula we count the number of fixed points of each element of G .

Label the beads 0, 1, 2, 3, 4, 5 in order counterclockwise around the bracelet. First we consider the six rotations in G . The identity I fixes all the elements of S , so I has 60 fixed points. Let R be rotation by $\pi/3$. The non-trivial rotations in G are R, R^2, R^3, R^4 , and R^5 , and these rotations act on the beads 0, 1, 2, 3, 4, 5 by $R^i(j) = i + j \pmod{6}$.

If an element of S is fixed by R , then every bead i must be the same color as the next bead $i + 1 \pmod{6}$, so all the beads must be the same color. But we have at most 3 beads of any given color, so no elements of S are fixed by R . The same reasoning applies to $R^5 = R^{-1}$.

If an element of S is fixed by R^2 , then beads 0, 2, 4 have the same color, and beads 1, 3, 5 have the same color. But there are only 2 white beads and 1 blue bead, so R^2 has no fixed points. The same reasoning applies to $R^4 = R^{-2}$.

If an element of S is fixed by R^3 , then beads 0 and 3 have the same color, 1 and 4 have the same color, and 2 and 5 have the same color. This can happen only if there's an even number of beads of each color, so R^3 has no fixed points.

Now we consider the six flips. There are three "vertex flips" with axis through a pair of opposite vertices, and three "edge flips" with axis through the midpoints of a pair of opposite edges. If the vertex flip F^v has axis through vertices k and $k + 3$, then F fixes these two vertices, F interchanges vertices $k + 1, k - 1$, and F interchanges vertices $k + 2, k - 2$. Thus vertices $k + 1$ and $k - 1$ must be the same color, and vertices $k + 2$ and $k - 2$ must be the same color. So one of the fixed vertices k and $k + 3$ must be blue, and the other fixed vertex must be red. (That's two choices.) Then vertex $k + 1$ can be red or white (two choices), and this determines the colors of the remaining three vertices. So in all there are $2 \times 2 = 4$ elements of S fixed by each of the three vertex flips F^v .

If the edge flip F^e has axis through the midpoint of the edge between vertices k and $k + 1$, then F^e interchanges k with $k + 1$, $k - 1$ with $k + 2$, and $k - 2$ with $k + 3$. So each of these

pairs of vertices must be the same color. But this is not possible, since there is only one blue bead. Thus F^e has no fixed points.

Now we apply Burnside's formula to count the number of different bracelets, which is the number of orbits of the action of G on S :

$$N = \frac{1}{|G|} \sum_{g \in G} \#\text{Fix}(g) = \frac{1}{12}(60 + 4 + 4 + 4) = \frac{1}{12}(72) = 6.$$

3. Let G be an abelian group, and let H be a subgroup. Suppose that there is a homomorphism $\varphi : G \rightarrow H$ such that $\varphi(h) = h$ for all $h \in H$. Let $K = \ker \varphi$. Prove that $G \cong H \times K$.

To prove that $G \cong H \times K$, we must show (1) H and K are normal subgroups of G , (2) $H \cap K = \{e\}$, and (3) $HK = G$.

(1) Since G is abelian, all subgroups of G are normal. Thus H and K are normal.

(2) Let $g \in H \cap K$. Since $g \in H$, we have $\phi(g) = g$. Since $g \in K$, we have $\phi(g) = e$. Thus $g = e$.

(3) Given $g \in G$, let $h = \phi(g) \in H$, and let $k = h^{-1}g$. Then $\phi(k) = \phi(h^{-1}g) = \phi(h^{-1})\phi(g) = (\phi(h))^{-1}\phi(g) = h^{-1}h = e$, so $k \in K$. Thus we have $g = h(h^{-1}g) = hk \in HK$.

4. Prove that if the group G has order 22 and G has only one element of order 2, then G is cyclic.

We present two solutions.

First solution: Since $|G| = 22$, every element of G has order a divisor of 22, namely 1, 2, 11, or 22. If we can find an element g of order 22, then $G = \langle g \rangle$, the cyclic group generated by g . Now the only element of order 1 is the identity e , and by hypothesis there is only one element a of order 2. By Sylow I, G has a Sylow 11-subgroup K , and $|K| = 11$. Let s be the number of Sylow 11-subgroups. By Sylow III, we have $s|22$ and $s \equiv 1 \pmod{11}$, so $s = 1$. Let $g \in G \setminus K$ with $g \neq a$. The order of g is not 1 since $g \neq e$. The order of g is not 2 since a is the only element of order 2. If the order of g is 11 then the cyclic subgroup $\langle g \rangle$ has order 11, and so $\langle g \rangle$ is a Sylow 11-subgroup not equal to K , which is not possible. Therefore g has order 22.

Second solution: Sylow I implies that G has a Sylow 2-subgroup H of order 2 and a Sylow 11-subgroup K of order 11. Since G has only one element of order 2 by hypothesis, there is only one Sylow 2-subgroup, and hence H is normal by Sylow II. By Sylow III, if s is the number of Sylow 11-subgroups, then $s|22$ and $s \equiv 1 \pmod{11}$, so $s = 1$. Sylow II implies that K is normal. [One can also deduce K is normal from $[G : K] = 2$.]

Now we prove that $G \cong H \times K$. We have just shown that H and K are normal. To see that $H \cap K = \{e\}$, note that $H \cap K$ is a subgroup of both H and K , so $|H \cap K|$ divides $|H| = 2$ and $|K| = 11$, so $|H \cap K| = 1$. It was proved in class that if H and K are normal and $H \cap K = \{e\}$, then HK is a subgroup of G . [Alternately, it is easy to show that for all subgroups H and K of an abelian group G , the product HK is a subgroup of G .] Thus $|HK|$ divides $|G| = 22$. Since H and K are subgroups of HK , we have that 2 divides $|HK|$ and 11 divides $|HK|$. Thus $|HK| = 22$, and so $HK = G$.

Since 2 and 11 are prime, we have $H \cong \mathbb{Z}_2$ and $K \cong \mathbb{Z}_{11}$, so $G \cong H \times K \cong \mathbb{Z}_2 \times \mathbb{Z}_{11} \cong \mathbb{Z}_{22}$, and so G is cyclic.

5. Find the Galois group of the field $K = \mathbb{Q}[\sqrt[6]{2}, i\sqrt{3}]$ over the rational numbers \mathbb{Q} . Show your reasoning.

First we prove that K is the splitting field of the polynomial $f(x) = x^6 - 2 \in \mathbb{Q}[x]$. Let $a = \sqrt[6]{2}$, and let $\omega = \frac{1}{2} + \frac{\sqrt{3}}{2}i$, a primitive sixth root of unity. The roots of $f(x)$ are $a, \omega a, \omega^2 a, \omega^3 a, \omega^4 a, \omega^5 a$. Now $a \in K$ and $\omega \in K$, so $f(x)$ splits in K . On the other hand, if a field K' contains all the roots of $f(x)$, then K' contains a and ωa , and so K' contains $\omega = \omega a/a$, and hence K' contains $i\sqrt{3}$. Thus K' is contained in K . Therefore K is the splitting field of $f(x)$.

Let $L = \mathbb{Q}[\sqrt[6]{2}]$. Then $[L : \mathbb{Q}] = 6$, since $\sqrt[6]{2}$ is a root of the polynomial $f(x) = x^6 - 2 \in \mathbb{Q}[x]$, and $f(x)$ is irreducible by Eisenstein's criterion. Also $[K : L] = 2$ since $i\sqrt{3}$ is a root of $g(x) = x^2 + 3 \in L[x]$, and $g(x)$ is irreducible in $L[x]$, because the roots of $g(x)$ are $\pm i\sqrt{3}$, which are not in L , since $L \subset \mathbb{R}$. Thus $[K : \mathbb{Q}] = [K : L][L : \mathbb{Q}] = 12$.

Since K is the splitting field of $x^6 - 2$, it follows that K is a Galois extension of \mathbb{Q} ; in other words, $|G(K/\mathbb{Q})| = [K : \mathbb{Q}] = 12$.

If $\phi \in G(K/\mathbb{Q})$, then $\phi(i\sqrt{3}) = \pm i\sqrt{3}$, since $i\sqrt{3}$ is a root of the polynomial $g(x) = x^2 + 3$, and the roots of $g(x)$ are $-1, i\sqrt{3}, -i\sqrt{3}$. Since $\omega = \frac{1}{2} + \frac{\sqrt{3}}{2}i$, we have $\phi(\omega) = \omega$ or $\phi(\omega) = \bar{\omega}$. If $\phi \in G(K/\mathbb{Q})$, then $\phi(a)$ is a root of $f(x)$, so $\phi(a) \in \{a, \omega a, \omega^2 a, \omega^3 a, \omega^4 a, \omega^5 a\}$. Since $\phi \in G(K/L)$ is determined by $\phi(a)$ and $\phi(i\sqrt{3})$, the 12 elements of $G(K/L)$ are:

$$\begin{aligned} \phi_0 : a &\mapsto a, \omega &\mapsto \omega \\ \phi_1 : a &\mapsto a, \omega &\mapsto \bar{\omega} \\ \phi_2 : a &\mapsto \omega a, \omega &\mapsto \omega \\ \phi_3 : a &\mapsto \omega a, \omega &\mapsto \bar{\omega} \\ \phi_4 : a &\mapsto \omega^2 a, \omega &\mapsto \omega \\ \phi_5 : a &\mapsto \omega^2 a, \omega &\mapsto \bar{\omega} \\ \phi_6 : a &\mapsto \omega^3 a, \omega &\mapsto \omega \\ \phi_7 : a &\mapsto \omega^3 a, \omega &\mapsto \bar{\omega} \\ \phi_8 : a &\mapsto \omega^4 a, \omega &\mapsto \omega \\ \phi_9 : a &\mapsto \omega^4 a, \omega &\mapsto \bar{\omega} \\ \phi_{10} : a &\mapsto \omega^5 a, \omega &\mapsto \omega \\ \phi_{11} : a &\mapsto \omega^5 a, \omega &\mapsto \bar{\omega} \end{aligned}$$

Now $\phi_0 = I$, the identity map. Let $F = \phi_1$ and $R = \phi_2$. Then $F^2 = I$, $R^6 = I$, and $FRF = R^{-1}$. In fact $\phi_{2n} = R^n$ and $\phi_{2n+1} = R^n F$ for $n = 0, 1, 2, 3, 4, 5$. Therefore $G(K/L) \cong D_6$.