Solutions

Exercise 1. Suppose G is a nonabelian group of order 8. In previous homework, you have shown that $G = AB$, where $A = \langle a \rangle$ is cyclic of order four and $B = \langle b \rangle$ is cyclic, generated by some element $b \in G - A$. Show that

a) $bab^{-1} = a^{-1}$.

b) If b has order two then $G \simeq D_4$.

c) If b has order four then $G \simeq Q_8$.

This completes the classification of non-abelian groups of order eight.

Proof. a) Since $[G : A] = 2$, we have $A \triangleleft G$. Hence $bab^{-1} \in A$. As bab^{-1} has the same order as a, we have $bab^{-1} = a$ or a^{-1}. Since G is nonabelian, we must have $bab^{-1} = a^{-1}$.

b) If b has order two then $G \simeq D_4$ by Homework 5, exercise 4.

c) Suppose b has order four. From the previous homework, the center of G has order 2, and if z is its nontrivial element, then $a^2 = b^2 = z$. Let $c = ab$. Since $a^{-1} = az$ and $b^{-1} = bz$, we have $ba = a^{-1}b = zab = zc$. Likewise, $bc = a, cb = za$ and $ca = b, ac = zb$. Hence there is an isomorphism $f : G \to Q_8$ such that $f(a) = i, f(b) = j, f(c) = k, f(z) = -1$. □

Exercise 2. In the previous homework, you showed that the polynomial

$$f(x) = x^4 - 10x^2 + 1$$

is irreducible in $\mathbb{Q}[x]$. Choose three primes p, and show that $\bar{f}(x)$ is reducible in $\mathbb{Z}_p[x]$ for each of your primes p.

(It turns out that $\bar{f}$ is reducible in $\mathbb{Z}_p[x]$ for every p.)

Proof. For $p = 2$, we have $\bar{f}(x) = x^4 + 1 = (x + 1)^4$.

For $p = 3$, we have $\bar{f}(x) = x^4 - x^2 + 1 = x^4 + 2x^2 + 1 = (x^2 + 1)^2$.

For $p = 5$, we have $\bar{f}(x) = x^4 + 1 = (x^2 + 2)(x^2 + 3)$.

For $p = 7$, we have $\bar{f}(x) = x^4 + 4x^2 + 1 = (x^2 - x - 1)(x^2 + x - 1)$.

For $p = 11$, we have $\bar{f}(x) = x^4 + x^2 + 1 = (x^2 - x + 1)(x^2 + x + 1)$.

□

Exercise 3. Find the minimal polynomial of $\sqrt{3} + \sqrt{5}$ in $\mathbb{Q}[x]$. This is similar to the last homework, but now use the Corollary to Gauss' Lemma to prove irreducibility.

Solution. The minimal polynomial is $f(x) = x^4 - 16x^2 + 4$. Using the rational root test, one checks there is no root in $\mathbb{Q}$. If $f(x)$ is reducible in $\mathbb{Q}[x]$, then by Gauss, it must factor as a product of two quadratic polynomials in $\mathbb{Z}[x]$. Since the coefficient of x^3 is zero, this factorization must be of the form

$$x^4 - 16x^2 + 4 = (x^2 + ax + b)(x^2 - ax + c),$$

where $bc = 4$, $a(c - b) = 0$, and $b + c + 16 = a^2$. If $a = 0$ then $b + c + 16 = 0$, which is impossible for integers b, c such that $bc = 4$. If $c - b = 0$, then $b = c = \pm 2$, so $a^2 = 20$ or $a^2 = 12$, both of which are impossible for an integer a. Hence $f(x)$ is irreducible.

□