Solutions

Exercise 1. Suppose G is a nonabelian group of order p^3. Prove that for any $a \in G$ we have $a^p \in Z(G)$. Hint: Recall the structure of $G/Z(G)$.

Proof. Let us write $Z = Z(G)$. From previous homework, we know that $G/Z \simeq \mathbb{Z}_p \times \mathbb{Z}_p$. Hence the p^{th} power of every element in G/Z is the identity coset, namely Z. Let $a \in G$. Then $Z = (aZ)^p = a^p Z$, so $a^p \in Z$, as desired. □

Exercise 2. Let G be a nonabelian group of order 8. We know $Z(G) \simeq \mathbb{Z}_2$. Let z be the nontrivial element of $Z(G)$. Prove that G contains elements of order 4, and that the square of any such element is z.

Proof. If $a^2 = 1$ for all $a \in G$ then G is abelian. If G has an element of order eight, then G is cyclic, and again abelian. Since G is nonabelian, it follows there must be an element $a \in G$ of order four. By the previous exercise, we have $a^2 \in Z(G)$. Since $a^2 \neq e$ and z is the unique nontrivial element of $Z(G)$, we must have $a^2 = z$. □

Exercise 3. Let G be a nonabelian group of order 8, let $a \in G$ be an element of order 4, let $A = \langle a \rangle$, let $b \in G$ be any element not in A, and let $B = \langle b \rangle$. Prove that $A \triangleleft G$ and $G = AB$.

Proof. Since A has index two in G, it is normal in G. Hence AB is a subgroup of G. We have $A \leq AB \leq G$. By Lagrange's theorem, we know that 4 divides $|AB|$, which in turn divides 8. Also $A \neq AB$, since b is not in A. It follows that $|AB| = 8 = |G|$, so $AB = G$. □

Exercise 4. Find all irreducible cubic and quartic polynomials in $\mathbb{Z}_2[x]$.

Solution. A polynomial $f(x) \in \mathbb{Z}_2[x]$ has no root in $\mathbb{Z}_2$ iff $f(0) = 1$ and f has an odd number of terms. It follows that the irreducible cubics are

$$x^3 + x + 1, \quad x^3 + x^2 + 1.$$

For a quartic to have no root in $\mathbb{Z}_2$ yet still be reducible, it must be a product of irreducible quadratic polynomials in $\mathbb{Z}_2[x]$. There is only one such polynomial, namely x^2+x+1, whose square is x^4+x^2+1. Hence the irreducible quartics are

$$x^4 + x + 1, \qquad x^4 + x^3 + 1, \qquad , x^4 + x^3 + x^2 + x + 1.$$

□

Exercise 5. Find a the irreducible polynomial of $\sqrt{2} + \sqrt{3}$ in $\mathbb{Q}[x]$.

Solution. Let $\alpha = \sqrt{2} + \sqrt{3}$. Then $\alpha^2 = 5 + 2\sqrt{6}$ and $(\alpha^2 - 5)^2 = 24$, so $\alpha^4 - 10\alpha^2 + 1 = 0$. Hence α is a root of the polynomial

$$f(x) = x^4 - 10\alpha^2 + 1 = 0.$$

It remains to show that $f(x)$ is irreducible in $\mathbb{Q}[x]$. The only possible rational roots are ± 1, which are not roots, so we have to show that $f(x)$ is not a product of two irreducible quadratics.

If we replace α by $\pm\sqrt{2} \pm \sqrt{3}$, the same polynomial arises, so these are the four roots of $f(x)$. If $q(x) = x^2 + ax + b$ is a quadratic factor of $f(x)$, then the sum of the two roots is $a \in \mathbb{Q}$, and their product is $b \in \mathbb{Q}$. The only way to have the sum in $\mathbb{Q}$ is if the roots are negatives of each other. But then their product involves $\sqrt{6}$, hence is not rational.

Alternatively, using Gauss' lemma, the two quadratic factors would have to be $x^2 \pm ax + b$, with $a \in \mathbb{Z}$ and $b = \pm 1$. To have the product of these equal $f(x)$ would lead to the equation $a^2 = 10 + 2b = 10 \pm 2$, which has no solution in integers. □

Exercise 6. This exercise is is about the roots (in $\mathbb{R}$) of the polynomial

$$f(x) = x^3 - 3x + 1.$$

a) Use the trigonometric identity $4\cos^3\theta - 3\cos\theta = \cos 3\theta$ to show that the roots of $f(x)$ are

$$2\cos\frac{2\pi}{9}, \quad 2\cos\frac{4\pi}{9}, \quad 2\cos\frac{8\pi}{9}.$$

b) Using part a), prove that

$$\cos\frac{2\pi}{9} + \cos\frac{4\pi}{9} + \cos\frac{8\pi}{9} = 0,$$

and

$$\cos\frac{2\pi}{9} \cdot \cos\frac{4\pi}{9} \cdot \cos\frac{8\pi}{9} = -\frac{1}{8}.$$

Proof. a) Multiply the identity by two and let $\theta = 2\pi/9$. We get

$$8\cos^3\frac{2\pi}{9} - 6\cos\frac{2\pi}{9} = 2\cos\frac{2\pi}{3} = -1,$$

or

$$(2\cos\frac{2\pi}{9})^3 - 3(2\cos\frac{2\pi}{9}) + 1 = 0,$$

so that $2\cos\frac{2\pi}{9}$ is a root of $f(x)$. Since $\cos\frac{2\pi}{3} = \cos\frac{4\pi}{3} = \cos\frac{8\pi}{3}$, the numbers $2\cos\frac{4\pi}{9}$ and $2\cos\frac{8\pi}{9}$ are also roots of $f(x)$.

b) For a general cubic polynomial $x^3 + ax^2 + bx + c$, with roots α, β, γ, we have

$$x^3 + ax^2 + bx + c = (x-\alpha)(x-\beta)(x-\gamma) = x^3 - (\alpha+\beta+\gamma)x^2 + (\alpha\beta + \beta\gamma + \gamma\alpha)x - \alpha\beta\gamma,$$

so

$$\begin{aligned} \alpha + \beta + \gamma &= -a \\ \alpha\beta + \beta\gamma + \gamma\alpha &= +b \\ \alpha\beta\gamma &= -c. \end{aligned}$$

In this case we have $a = 0$ and $c = 1$, so

$$2\cos\frac{2\pi}{9} + 2\cos\frac{4\pi}{9} + 2\cos\frac{8\pi}{9} = 0$$

and

$$2^3 \cdot \cos\frac{2\pi}{9} \cdot \cos\frac{4\pi}{9} \cdot \cos\frac{8\pi}{9} = -1.$$

$\square$