Solutions

Exercise 1. Suppose G is a nonabelian group of order p^3. We have seen that the center $Z = Z(G)$ has order p. Let $a \in G$, but $a \notin Z$.

a) Prove that for all $b \in G$, we have $a^{-1}bab^{-1} \in Z$. (See exam 2, problem 3).

b) Prove that the map $f_a : G \to Z$ given by $f_a(b) = a^{-1}bab^{-1}$ is a surjective group homomorphism, with $\ker f_a$ equal to the centralizer $C_G(a)$ of a.

c) Prove that the conjugacy class of a in G is the coset aZ.

d) How many conjugacy-classes of each order does G have?

Proof. a) In exam 2, you showed that if G/H is abelian then $xyx^{-1}y^{-1} \in H$ for all $x, y \in G$. In this case, we have $G/Z \simeq \mathbb{Z}_p \times \mathbb{Z}_p$ abelian, so a) holds.

b) We compute

$$f_a(bc) = a^{-1}(bc)a(bc)^{-1} = a^{-1}bcac^{-1}b^{-1} = a^{-1}ba \cdot a^{-1}cac^{-1} \cdot b^{-1} = a^{-1}ba \cdot f_a(c) \cdot b^{-1}.$$

Since $f_a(c) \in Z$, by part a), we have

$$f_a(bc) = a^{-1}bab^{-1} \cdot f_a(c) = f_a(b)f_a(c),$$

so f_a is a group homomorphism. Since $a \notin Z$, the image of f_a is a nontrivial subgroup of Z. Since $|Z| = p$, the image of f_a equals Z. That is, f_a is surjective. Its kernel is determined as follows.

$$\ker f_a = \{b \in G : \ a^{-1}bab^{-1} = e\} = \{b \in G : \ bab^{-1} = a\} = C_G(a).$$

c) The conjugacy-class of a is $\{bab^{-1} : \ b \in G\} = \{a \cdot f_a(b) : \ b \in G\} = a\{f_a(b) : \ b \in G\} = aZ$.

d) From c), the $p^3 - p$ noncentral elements of G are partitioned into conjugacy-classes of size p. And each element of Z is alone in its conjugacy class. Hence there are $p^2 - 1$ conjugacy classes of size p and p conjugacy classes consisting of one element. □

Exercise 2. In homework 6, you showed that the set of matrices

$$F = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \right\}$$

under matrix addition and multiplication, is a field. We have also seen that $\mathbb{Z}_2[x]$ has a unique quadratic polynomial, namely $x^2 + x + 1$. Prove that

$$\mathbb{Z}_2[x]/(x^2 + x + 1) \simeq F.$$

Proof. The matrix $\alpha = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$ satisfies $\alpha^2 + \alpha + 1 = 0$. The polynomial $x^2 + x + 1$ is irreducible in $\mathbb{Z}_2[x]$, so it generates the kernel of the homomorphism

$$\phi_\alpha : \mathbb{Z}_2[x] \to F, \qquad \phi_\alpha(f) = f(\alpha).$$

Since $F = \{0, 1, \alpha, \alpha^2\}$, the ring homomorphism ϕ_α is surjective. From the First Isomorphism Theorem, we get an isomorphism

$$\bar{\phi}_\alpha : \mathbb{Z}_2[x]/(x^2 + x + 1) \xrightarrow{\sim} F.$$

□

Exercise 3. Let F be a field, and let $f(x) \in F[x]$ be a polynomial of degree $n \geq 1$, generating the ideal $(f) = \{gf : \ g \in F[x]\}$. Prove that each coset in $F[x]/(f)$ contains a unique polynomial of degree $< n$.

Proof. The ideal (f) is unchanged if we divide f by its coefficient of x^n. Hence we may assume that f is monic:

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

It suffices to prove by induction on $k \geq 0$ that

$$x^{n+k} \in h_k(x) + (f),$$

where $h_k(x) \in F[x]$ has degree $< n$. For $k = 0$, we have

$$x^n = -a_{n-1}x^{n-1} - \cdots - a_1 x - a_0 + f(x),$$

so the claim holds, with $h_0(x) = -a_{n-1}x^{n-1} - \cdots - a_1 x - a_0$. Assume that $x^{n+k-1} \in h_{k-1}(x) + (f)$, where $h_{k-1}(x) \in F[x]$ has degree $< n$. Write

$$h_{k-1}(x) = c_{n-1}x^{n-1} + \ell(x),$$

where $\deg \ell(x) < n - 1$. Then

$$x^{n+k} \in x h_{k-1}(x) + (f) = c_{n-1}x^n + x\ell(x) + (f) = c_{n-1}h_0(x) + x\ell(x) + (f).$$

Thus, we have $x^{n+k} \in h_k(x) + (f)$, where $h_k(x) = c_{n-1}h_0(x) + x\ell(x)$. Since $h_0(x)$ and $x\ell(x)$ both have degree $< n$, it follows that $\deg h_k < n$, so the claim is proved by induction.

As for uniqueness, suppose $g+(f) = h+(f)$ with both g and h having degrees $< n$. Then $g-h \in (f)$, so f divides the polynomial $g - h$ of degree $< n$. Since $\deg f = n$, this can only hold if $g - h = 0$, that is, if $g = h$.

□