QUESTION 16

Let G be a finite abelian group of order n, and let m be a positive integer relative prime to n. Then the mapping $\sigma: x \to x^m$ is an automorphism of G.

Solution:

(m,n) = 1 ⇒ there exist integers u and v such that mu + nv = 1 ⇒ for all $x \in G$, $x^{mu+nv} = x^{mu}\, x^{nv} = x^{um}$ since o(G)=n.

Now for all $x \in G$, $x=(x^u)^m$ implies that σ is onto. Further,

$x^m = e \Rightarrow x^{mu} = e \Rightarrow x = e$, showing that σ is 1-1.

That σ is a homomorphism follows from the fact that G is abelian. Hence, σ is an automorphism of G.

QUESTION 17

Let $G = \langle a \mid a^n = e \rangle$ be a finite cyclic group of order n. Then the mapping $\sigma : a \to a^m$ is an automorphism of G iff (m,n) = 1.Further, if (m,n)=d, then $(a^m)^{n/d} = (a^n)^{m/d} = e$. Thus, the order of a^m divides n/d; that is, n|n/d. Hence, d = 1, and the solution is complete.Let X be a G-set. Then G_x is a subgroup of G for each $x \in X$.

Proof:

Let $x \in X$ and let $g_1, g_2 \in G_x$. Then $g_1x=x$ and $g_2x=x$. Consequently, $(g_1g_2)x=g_1(g_2x)=g_1x=x$, so $g_1g_2 \in G_x$, and G_x is closed under the induced operation of G. Of course $ex=x$, so $e \in G_x$. If $g \in G_x$, then $gx = x$, so $x=ex=(g^{-1}g)x= g^{-1}(gx)=g^{-1}x$, and consequently $g^{-1} \in G_x$. Thus G_x is a subgroup of G.

QUESTION 18

Let X be a G-set. For x_1, $x_2 \in X$, let $x_1 \sim x_2$ if and only if there exists $g \in G$ such that $gx_1 = x_2$. Then $\sim$ is an equivalence relation on X.

Proof:

For each $x \in X$, we have $ex = x$, so $x \sim x$ and $\sim$ is reflexive.

Suppose $x_1 \sim x_2$, so $gx_1 = x_2$ for some $g \in G$. Then $g^{-1}x_2 = g^{-1}(gx_1) = (g^{-1}g)x_1 = ex_1 = x_1$, so $x_2 \sim x_1$, and $\sim$ is symmetric. Finally, if $x_1 \sim x_2$ and $x_2 \sim x_3$, then $g_1x_1 = x_2$ and $g_2x_2 = x_3$ for some $g_1, g_2 \in G$. Then $(g_2g_1)x_1 = g_2(g_1x_1) = g_2x_2 = x_3$, so $x_1 \sim x_3$ and $\sim$ is transitive.

QUESTION 19

If N is a normal subgroup of G, and if H is any subgroup of G, then

H V N=HN=NH. Furthermore, if H is also normal in G, then HN is normal in G.

Proof:

We show that HN is a subgroup of G, from which

H V N=HN follows at once. Let $h_1, h_2 \in H$ and $n_1, n_2 \in N$. Since N is a normal subgroup, we have $n_1 h_2 = h_2 n_3$ for some $n_3 \in N$. Then $(h_1 n_1)(h_2 n_2) = h_1(n_1 h_2)n_2 = h_1(h_2 n_3)n_2 = (h_1 h_2)(n_3 n_2) \in HN$, so HN is closed under the induced operation in G. Clearly $e=ee$ is in HN. For $h \in H$ and $n \in N$, we have $(hn)^{-1} = n^{-1} h^{-1} = h^{-1} n_4$ for some $n_4 \in N$, since N is a normal subgroup. Thus $(hn)^{-1} \in HN$, so $HN \leq G$.

A similar argument shows that NH is a subgroup, so NH=H V N=HN.

Now suppose that H is also normal in G, and let $h \in H$, $n \in N$, and $g \in G$. Then

$ghng^{-1} = (ghg^{-1})(gng^{1}) \in HN$, so HN is indeed normal in G.

QUESTION 20

Let G be a group such that for some fixed integer n >1, $(ab)^n = a^n b^n$ for all a, b∈G. Let $G_n = \{a \in G \mid a^n = e\}$ and $G^n = \{a^n \mid a \in G\}$. Then $G_n \lhd G$, $G^n \lhd G$, and $G/G_n \simeq G^n$.

Solution:

Let a, b∈G_n and x∈G. Then $(aba^{-1})^n = a^n (b^n)^{-1} = e$, so $aba^{-1} \in G_n$. Also, $(xax^{-1})^n = (xax^{-1})\ldots(xax^{-1}) = xa^n x^{-1} = e$ implies $xax^{-1} \in G_n$. Hence, $G_n \lhd G$.

Let a, b, x∈G. Then $a^n (b^n)^{-1} = (aba^{-1})^n \in G^n$.

Also, $xa^n x^{-1} = (xax^{-1})\ldots(xax^{-1}) = (xax^{-1})^n \in G^n$. Therefore, $G^n \lhd G$.

QUESTION 21

Third Isomorphism Theorem

Let H and K be normal subgroups of a group G with $K \leq H$. Then $G/H \simeq (G/K)/(H/K)$.

Proof:

Let $\phi: G \to (G/K)/(H/K)$ be given by $\phi(a) = (aK)(H/K)$ for $a \in G$. Clearly ϕ is onto $(G/K)/(H/K)$, and for $a, b \in G$,

$\phi(ab) = [(ab)K](H/K)$

$= [(aK)(bK)](H/K)$

$= [(aK)(H/K)][(bK)(H/K)] = \phi(a)\,\phi(b)$, so ϕ is a homomorphism.

The kernel consists of those $x \in G$ such that $\phi(x) = H/K$.

These x are just the elements of H.

Then first isomorphism theorem shows that $G/H \simeq (G/K)/(H/K)$.

QUESTION 22

Let G be a group of order p^n and let X be a finite G-set. Then

$|X| \equiv |X_G| \pmod{p}$.

Proof:

Recall $|X| = |X_G| + \sum_{i=s+1}^{r} |Gx_i|$. In the notation of above Equation,

we know that

$|Gx_i|$ divides $|G|$.

Consequently p divides $|Gx_i|$ for $s + 1 \leq i \leq r$. Above equation then shows that $|X| - |X_G|$ is divisible by p, so $|X| \equiv |X_G| \pmod{p}$.

QUESTION 23

Let H be a p-subgroup of a finite group G. Then

$$(N[H]:H) \equiv (G:H) \pmod{p}.$$

Proof:

Let $\mathcal{L}$ be the set of left cosets of H in G, and let H act on $\mathcal{L}$ by left translastion, so that h(xH) = (hx)H. Then $\mathcal{L}$ becomes an H-set. Note that $|\mathcal{L}|=(G:H)$. Let us determine $\mathcal{L}_H$, that is, those left cosets that are fixed under action by all elements of H. Now xH= h(xH) if and only if $H=x^{-1}hxH$, or if and only if $x^{-1}hx \in H$.

Thus xH=h(xH) for all h∈H if and only if $x^{-1}hx = x^{-1}h(x^{-1})^{-1} \in H$ for all h∈H, or if and only if $x^{-1} \in N[H]$, or if and only if x∈N[H]. Thus the left cosets in $\mathcal{L}_H$ are those contained in N[H]. The number of such cosets is (N[H]:H), so $|\mathcal{L}_H| = (N[H]:H)$.

Since H is a p-group, it has order a power of p. Then $|\mathcal{L}| \equiv |\mathcal{L}_H| \pmod{p}$, that is, $(G:H) \equiv (N[H]:H) \pmod{p}$.

QUESTION 24

Second Sylow Theorem

Let P_1 and P_2 be Sylow p-subgroups of a finite group G. Then P_1 and P_2 are conjugate subgroups of G.

Proof:

Here we will let one of the subgroups act on left cosets of the other. Let $\mathcal{L}$ be the collection of left cosets of P_1, and let P_2 act on $\mathcal{L}$ by $z(xP_1)=(zx)P_1$ for $z\in P_2$. Then $\mathcal{L}$ is a P_2-set. We have $|\mathcal{L}_{P_2}| \equiv |\mathcal{L}| \pmod p$, and $|\mathcal{L}|= (G: P_1)$ is not divisible by p, so $|\mathcal{L}_{P_2}|\neq 0$. Let $xP_1 \in \mathcal{L}_{P_2}$.

Then $zxP_1=xP_1$ for all $z\in P_2$, so $x^{-1}zxP_1=P_1$ for all $z\in P_2$. Thus $x^{-1}zx\in P_1$ for all $z\in P_2$, so $x^{-1}P_2x\leq P_1$. Since $|P_1|=|P_2|$, we must have $P_1=x^{-1}P_2x$, so P_1 and P_2 are indeed conjugate subgroups.

QUESTION 25

The center of a finite nontrivial p-group G is nontrivial.

Proof:

We have $|G|=c+n_{c+1}+\ldots+n_r$, where n_i is the number of elements in the ith orbit of G under conjugation by itself.

For G, each n_i divides $|G|$ for $c+1 \leq i \leq r$, so p divides each n_i, and p divides $|G|$. Therefore p divides c. Now $e \in Z(G)$, so $c \geq 1$. Therefore $c \geq p$, and there exists some $a \in Z(G)$ where $a \neq e$.

QUESTION 26

For a prime number p, every group G of order p^2 is abelian.

Proof:

If G is not cyclic, then every element except e must be of order p.

Let a be such an element. Then the cyclic subgroup <a> of order p does not exhaust G. Also let $b \in G$ with $b \notin \langle a \rangle$. Then $\langle a \rangle \cap \langle b \rangle = \{e\}$, since an element c in $\langle a \rangle \cap \langle b \rangle$ with $c \neq e$ would generate both <a> and <b>, giving $\langle a \rangle = \langle b \rangle$, contrary to construction.

From first Sylow theorem, <a> is normal in some subgroup of order p^2 of G, that is, normal in all of G. Likewise <b> is normal in G.

Now <a> V <b> is a subgroup of G properly containing <a> and of order dividing p^2. Hence <a> V <b> must be all of G.

Thus the hypotheses of last lemma are satisfied, and G is isomorphic to <a> x <b> and therefore abelian.