Algebra I: Final 2015

June 24, 2015

ID#: **Name:**

Quote the following when necessary.

A. Subgroup H of a group G:

$$H \leq G \Leftrightarrow \emptyset \neq H \subseteq G,\ xy \in H \text{ and } x^{-1} \in H \text{ for all } x, y \in H.$$

B. Order of an Element: Let g be an element of a group G. Then $\langle g \rangle = \{g^n \mid n \in \boldsymbol{Z}\}$ is a subgroup of G. If there is a positive integer m such that $g^m = e$, where e is the identity element of G, $|g| = \min\{m \mid g^m = e,\ m \in \boldsymbol{N}\}$ and $|g| = |\langle g \rangle|$. Moreover, for any integer n, $|g|$ divides n if and only if $g^n = e$.

C. Lagrange's Theorem: If H is a subgroup of a finite group G, then $|G| = |G : H||H|$.

D. Normal Subgroup: A subgroup H of a group G is normal if $gHg^{-1} = H$ for all $g \in G$. If H is a normal subgroup of G, then G/H becomes a group with respect to the binary operation $(gH)(g'H) = gg'H$.

E. Direct Product: If $\gcd(m, n) = 1$, then $\boldsymbol{Z}_{mn} \approx \boldsymbol{Z}_m \oplus \boldsymbol{Z}_n$ and $U(mn) \approx U(m) \oplus U(n)$.

F. Isomorphism Theorem: If $\alpha : G \to \overline{G}$ is a group homomorphism, $\mathrm{Ker}(\alpha) = \{x \in G \mid \alpha(x) = e_{\overline{G}}\}$, where $e_{\overline{G}}$ is the identity element of $\overline{G}$. Then $G/\mathrm{Ker}(\alpha) \approx \alpha(G)$.

G. Sylow's Theorem: For a finite group G and a prime p, let $\mathrm{Syl}_p(G)$ denote the set of Sylow p-subgroups of G. Then $\mathrm{Syl}_p(G) \neq \emptyset$. Let $P \in \mathrm{Syl}_p(G)$. Then $|\mathrm{Syl}_p(G)| = |G : N(P)| \equiv 1 \pmod{p}$, where $N(P) = \{x \in G \mid xPx^{-1} = P\}$.

Other Theorems: List other theorems you applied in your solutions.

Please write your message: Comments on group theory. Suggestions for improvements of this course. Write on the back of this sheet is also welcome.

1. Let H and K be subgroups of a group G. Let $a, b \in G$. Show the following. (20 pts)

   (a) $aH = bH$ if and only if $a^{-1}b \in H$.

   (b) $aKa^{-1} \leq G$ and $H \cap aKa^{-1} \leq H$.

   (c) For $x, y \in H$, $xaK = yaK$ if and only if $x^{-1}y \in H \cap aKa^{-1}$.

   (d) If $|H|$ and $|K|$ are finite, then $|HaK| = |H : H \cap aKa^{-1}||K|$.

2. Let $\phi : G \to H$ be an onto group homomorphism, e_G is the identity element of G and e_H the identity element of H. Show the following. (20 pts)

   (a) $\phi(e_G) = e_H$ and for $a \in G$, $\phi(a^{-1}) = \phi(a)^{-1}$.

   (b) $\mathrm{Ker}\phi = \{x \in G \mid \phi(x) = e_H\}$ is a normal subgroup of G.

   (c) The homomorphism ϕ is an isomorphism if and only if $\mathrm{Ker}\phi = \{e_G\}$.

   (d) If G is Abelian, then H is Abelian.

3. Answer the following questions on Abelian groups of order $675 = 3^3 \cdot 5^2$. (20 pts)

   (a) Using the Fundamental Theorem of Finite Abelian Groups, list all non-isomorphic Abelian groups of order 675.

   (b) Explain that every Abelian group of order 675 has at least 8 elements of order 15.

   (c) If an Abelian group of order 675 has at most 8 elements of order 15, then it is cyclic.

   (d) Let $G = \boldsymbol{Z}_9 \oplus \boldsymbol{Z}_{75}$. Find the number of subgroups of G of order 15.

4. Let $G = \langle a \rangle$ be a cyclic group of finite order n. Show the following. (20 pts)

   (a) $\sigma : \boldsymbol{Z} \to G$ ($i \mapsto a^i$). Then σ is an onto homomorphism and $\boldsymbol{Z}/n\boldsymbol{Z} \approx G$, where $n\boldsymbol{Z}$ is the set of integers divisible by n.

   (b) Let H be a subgroup of G of order m, and $n = mh$. Then $H = \langle a^h \rangle$.

   (c) $\langle a^i \rangle = G$ if and only if $\gcd(i, n) = 1$.

   (d) For $x \in U(n)$, let $\sigma_x : G \to G$ ($a^i \mapsto a^{xi}$). Then $\sigma_x \in \mathrm{Aut}(G)$, and $\phi : U(n) \to \mathrm{Aut}(G)$ ($x \mapsto \sigma_x$) is a group isomorphism.

5. Suppose p and q are prime numbers with $p > q$, and G is a group of order pq. Let $P \in \mathrm{Syl}_p(G)$ and $Q \in \mathrm{Syl}_q(G)$. Show the following. (20 pts)

   (a) P is a normal subgroup of G.

   (b) If Q is a normal subgroup, then G is cyclic.

   (c) If Q is not a normal subgroup, then $p \equiv 1 (\mathrm{mod}\ q)$ and $U(p)$ has a subgroup of order q.

   (d) Let $p = 11$ and $q = 5$. Find an element $r \in U(11)$ of order 5. Let $N = \langle a \rangle$ be a cyclic group of order 11 and $H = \{1, r, r^2, r^3, r^4\}$. Set $G = N \times H$. Then G is a non-Abelian group of order 55 with respect to the following binary operation:

$$G \times G \to G \ ((a^h, r^i)(a^j, r^k) \mapsto (a^{h+r^i j}, r^{i+k})), \text{ where } 0 \leq h, j \leq 10, \ 0 \leq i, k \leq 4.$$

Algebra I: Solutions to Final 2015

June 24, 2015

1. Let H be a subgroup of a group G. Let $a, b \in G$. Show the following. (20 pts)

   (a) $aH = bH$ if and only if $a^{-1}b \in H$.

   Soln. Since $H \leq G$, $H \neq \emptyset$. Let $a \in H$. Then $a^{-1} \in H$ and $e = aa^{-1} \in H$.

   Suppose $aH = bH$. Since $e \in H$, $aH = bH$ implies that $b = be \in bH = aH$. Hence there exists $h \in H$ such that $b = ah$. Therefore by multiplying a^{-1} to both hand sides from the left, $a^{-1}b = h \in H$.

   Conversely let $a^{-1}b = h \in H$. Then $b = ah$ and

   $$bH = ahH \subseteq aH = aeH = ahh^{-1}H = aa^{-1}bh^{-1}H \subseteq bH.$$

   Therefore $aH = bH$. ■

   (b) $aKa^{-1} \leq G$ and $H \cap aKa^{-1} \leq H$.

   Soln. Clearly, $e = aea^{-1} \in aKa^{-1}$ and $aKa^{-1} \neq \emptyset$. Let $k, k' \in K$. Since $K \leq G$, $kk' \in K$ and $k^{-1} \in K$ by (A). Hence $(aka^{-1})(ak'a^{-1}) = akk'a^{-1} \in aKa^{-1}$ and $(aka^{-1})^{-1} = ak^{-1}a^{-1} \in aKa^{-1}$. Thus by (A), $aKa^{-1} \leq G$. Clearly $e \in H \cap aKa^{-1} \subseteq H$. Since both H and aKa^{-1} are subgroups of G, $x, y \in H \cap aKa^{-1}$ implies $xy \in H \cap aKa^{-1}$ and $x^{-1} \in H \cap aKa^{-1}$. Thus $H \cap aKa^{-1} \leq H$. ■

   (c) For $x, y \in H$, $xaK = yaK$ if and only if $x^{-1}y \in H \cap aKa^{-1}$ by (A).

   Soln. Since $aKa^{-1} \leq G$ and $xaK = yaK \Leftrightarrow x(aKa^{-1}) = y(aKa^{-1})$, we can apply (a) to have the following; for $x, y \in H$

   $$xaK = yaK \Leftrightarrow x(aKa^{-1}) = y(aKa^{-1}) \Leftrightarrow x^{-1}y \in aKa^{-1}.$$

   Since $x, y \in H$, this is equivalent to the condition $x^{-1}y \in H \cap aKa^{-1}$. ■

   (d) If $|H|$ and $|K|$ are finite, then $|HaK| = |H : H \cap aKa^{-1}||K|$.

   Soln. Since HaK is a union of left cosets haK with $h \in H$. Since $|haK| = |K|$ and there are $|H : H \cap aKa^{-1}|$ many distinct left cosets of this type by (c), $|HaK| = |H : H \cap aKa^{-1}||K|$. ■

2. Let $\phi : G \to H$ be an onto group homomorphism, e_G is the identity element of G and e_H the identity element of H. Show the following. (20 pts)

   (a) $\phi(e_G) = e_H$ and for $a \in G$, $\phi(a^{-1}) = \phi(a)^{-1}$.

   Soln. $\phi(e_G) = \phi(e_G)^{-1}\phi(e_G)\phi(e_G) = \phi(e_G)^{-1}\phi(e_Ge_G) = \phi(e_G)^{-1}\phi(e_G) = e_H$. $\phi(a^{-1}) = \phi(a^{-1})\phi(a)\phi(a)^{-1} = \phi(a^{-1}a)\phi(a)^{-1} = \phi(e_G)\phi(a)^{-1} = e_H\phi(a)^{-1} = \phi(a)^{-1}$. ■

   (b) $\mathrm{Ker}\phi = \{x \in G \mid \phi(x) = e_H\}$ is a normal subgroup of G.

   Soln. Let $a, b \in \mathrm{Ker}\phi$. Then $\phi(ab) = \phi(a)\phi(b) = e_He_H = e_H$. Hence $ab \in \mathrm{Ker}\phi$. By (a) $\phi(a^{-1}) = \phi(a)^{-1} = e_H^{-1} = e_H$. Hence $a^{-1} \in \mathrm{Ker}\phi$. Thus $\mathrm{Ker}\phi$ is a subgroup of G. Let $g \in G$, then $\phi(gag^{-1}) = \phi(g)\phi(a)\phi(g^{-1}) = \phi(g)e_H\phi(g)^{-1} = e_H$. Hence $g\mathrm{Ker}\phi g^{-1} \subseteq \mathrm{Ker}\phi$ for all $g \in G$. Since this holds for $g^{-1} \in G$, $g^{-1}\mathrm{Ker}\phi g \subseteq \mathrm{Ker}\phi$, which implies $\mathrm{Ker}\phi \subseteq g\mathrm{Ker}\phi g^{-1}$. Thus $g\mathrm{Ker}\phi g^{-1} = \mathrm{Ker}\phi$ for all $g \in G$ and $\mathrm{Ker}\phi$ is a normal subgroup of G. ■

(c) The homomorphism ϕ is an isomorphism if and only if $\text{Ker}\phi = \{e_G\}$.

Soln. Since ϕ is onto, it suffices to show that ϕ is one-to-one. Oberve that

$$\phi(x) = \phi(y) \Leftrightarrow \phi(x)^{-1}\phi(y) = \phi(x^{-1}y) = e_H \Leftrightarrow x^{-1}y \in \text{Ker}\phi.$$

Hence if $\text{Ker}\phi = \{e_G\}$, $\phi(x) = \phi(y)$ implies $x = y$, and ϕ is one-to-one. Suppose it is one-to-one. Let $x = e$. Then $y \in \text{Ker}\phi$ implies $\phi(y) = \phi(e_G)$. Hence if ϕ is one-to-one, $y = e$ and $\text{Ker}\phi = \{e_G\}$ by (a). ■

(d) If G is Abelian, then H is Abelian.

Soln. Let $h, k \in H$. Since ϕ is onto, there are $a, b \in G$ such that $h = \phi(a)$ and $k = \phi(b)$. Now

$$hk = \phi(a)\phi(b) = \phi(ab) = \phi(ba) = \phi(b)\phi(a) = kh.$$

Therefore, H is Abelian. ■

3. Answer the following questions on Abelian groups of order $675 = 3^3 \cdot 5^2$. (20 pts)

(a) Using the Fundamental Theorem of Finite Abelian Groups, list all non-isomorphic Abelian groups of order 675.

Soln. Let φ be the Euler's phi function, i.e., $\varphi(n) = |U(n)|$. Since $\varphi(3) = 2$ and $\varphi(5) = 4$, the following holds

$G(3) \oplus G(5)$	Max Cyclic	Order 3	Order 5	Order 15
$\boldsymbol{Z}_{27} \oplus \boldsymbol{Z}_{25}$	$\boldsymbol{Z}_{675}$	2	4	8
$\boldsymbol{Z}_{27} \oplus \boldsymbol{Z}_5 \oplus \boldsymbol{Z}_5$	$\boldsymbol{Z}_5 \oplus \boldsymbol{Z}_{135}$	2	24	48
$\boldsymbol{Z}_9 \oplus \boldsymbol{Z}_3 \oplus \boldsymbol{Z}_{25}$	$\boldsymbol{Z}_3 \oplus \boldsymbol{Z}_{225}$	8	4	32
$\boldsymbol{Z}_9 \oplus \boldsymbol{Z}_3 \oplus \boldsymbol{Z}_5 \oplus \boldsymbol{Z}_5$	$\boldsymbol{Z}_{15} \oplus \boldsymbol{Z}_{45}$	8	24	192
$\boldsymbol{Z}_3 \oplus \boldsymbol{Z}_3 \oplus \boldsymbol{Z}_3 \oplus \boldsymbol{Z}_{25}$	$\boldsymbol{Z}_3 \oplus \boldsymbol{Z}_3 \oplus \boldsymbol{Z}_{75}$	26	4	104
$\boldsymbol{Z}_3 \oplus \boldsymbol{Z}_3 \oplus \boldsymbol{Z}_3 \oplus \boldsymbol{Z}_5 \oplus \boldsymbol{Z}_5$	$\boldsymbol{Z}_3 \oplus \boldsymbol{Z}_{15} \oplus \boldsymbol{Z}_{15}$	26	24	624

(b) Explain that every Abelian group of order 675 has at least 8 elements of order 15.

Soln. Since G is Abelian, for each divisor m of its order, there is a subgroup of order m. Since the only Abelian group of order 15 is cyclic, there is an element of order 15. Since $\varphi(15) = \varphi(3)\varphi(5) = 2 \cdot 4 = 8$, there are 8 elements of order 8 in a cyclic group of order 15. Therefore, there are at least 8 elements of order 15. See the above table. ■

(c) If an Abelian group of order 675 has at most 8 elements of order 15, then it is cyclic.

Soln. If it is not cyclic, then there are at least two subgroups of order 3 or there are at least two subgroups of order 5. Hence there are more than one subgroup of order 15. Since each subgroup of order 15 contains at least 8 elements of order 8, there are more than 8 elements of order 15 in this case. Therefore the assertion holds. See the above table. ■

(d) Let $G = \boldsymbol{Z}_9 \oplus \boldsymbol{Z}_{75}$. Find the number of subgroups of G of order 15.

Soln. Since $\boldsymbol{Z}_9 \oplus \boldsymbol{Z}_{75} \approx \boldsymbol{Z}_9 \oplus \boldsymbol{Z}_3 \oplus \boldsymbol{Z}_{25}$ contains $3^2 - 1 = 8$ elements of order 3 and $5^1 - 1 = 4$ elements of order 5. Therefore it contains 32 elements of order 15. Each subgroup of order 15 contains $\varphi(15) = 8$ elements of order 15, and each element of order 15 is contained in exactly one subgroup of order 15, there are $32/8 = 4$ subgroups of order 15. ■

4. Let $G = \langle a \rangle$ be a cyclic group of finite order n. Show the following. (20 pts)

   (a) $\sigma : \boldsymbol{Z} \to G$ $(i \mapsto a^i)$. Then σ is an onto homomorphism and $\boldsymbol{Z}/n\boldsymbol{Z} \approx G$, where $n\boldsymbol{Z}$ is the set of integers divisible by n.

   Soln. Since $G = \langle a \rangle = \{a^i \mid i \in \boldsymbol{Z}\}$, σ is onto. $\sigma(i+j) = a^{i+j} = a^i a^j = \sigma(i)\sigma(j)$, σ is a group homomorphism. Ker$\sigma = n\boldsymbol{Z}$ because by (B)

   $$m \in \mathrm{Ker}\sigma \Leftrightarrow a^m = e \Leftrightarrow n \mid m \Leftrightarrow m \in n\boldsymbol{Z}.$$

   Thus by (F), $\boldsymbol{Z}/n\boldsymbol{Z} \approx G$. ■

   (b) Let H be a subgroup of G of order m, and $n = mh$. Then $H = \langle a^h \rangle$. Since G is cyclic, there is only one subgroup of order m. Hence $H = \langle a^h \rangle$.

   Soln. By (B), $|a^h| = m$. Hence $\langle a^h \rangle$ is a subgroup of order m. ■

   (c) $\langle a^i \rangle = G$ if and only if $\gcd(i, n) = 1$.

   Soln. Clearly $\langle a^i \rangle \subseteq G$. If $\gcd(i, n) = 1$, there are $s, t \in \boldsymbol{Z}$ such that $is + nt = 1$. Hence $a = a^1 = a^{is+nt} = (a^i)^s(a^n)^t = (a^i)^s \in \langle a^i \rangle$. Therefore $\langle a \rangle \subseteq \langle a^i \rangle$ and $\langle a^i \rangle = G$. If $\langle a^i \rangle = G$, $a = (a^i)^s$ for some $s \in \boldsymbol{Z}$. Then by (B), $n \mid is - 1$. Therefore, there is $t \in \boldsymbol{Z}$ such that $is - 1 = nt$, and $is - nt = 1$. Let $d = \gcd(i, n)$. Since $d \mid i$ and $d \mid n$, $d \mid is - nt = 1$. Therefore, $d = 1$. ■

   (d) For $x \in U(n)$, let $\sigma_x : G \to G$ $(a^i \mapsto a^{xi})$. Then $\sigma_x \in \mathrm{Aut}(G)$, and $\phi : U(n) \to \mathrm{Aut}(G)$ $(x \mapsto \sigma_x)$ is a group isomorphism.

5. Suppose p and q are prime numbers with $p > q$, and G is a group of order pq. Let $P \in \mathrm{Syl}_p(G)$ and $Q \in \mathrm{Syl}_q(G)$. Show the following. (20 pts)

   (a) P is a normal subgroup of G.

   Soln. By (G), $|\mathrm{Syl}_p(G)| = |G : N(P)| \equiv 1 (\mathrm{mod}\ p)$. By (C), $|G : N(P)|$ is a divisor of pq and 1 modulo p. Hence it is either 1 or q. Since $q < p$, $p \nmid q - 1$ and $q \not\equiv 1$ (mod p). Therefore $|G : N(P)| = 1$ and $G = N(P) = \{x \in G \mid xPx^{-1} = P\}$. Hence $P \lhd G$. ■

   (b) If Q is a normal subgroup, then G is cyclic.

   Soln. By 1(d) with $H = P$, $a = e$ and $K = Q$, $|PQ| = |P : P \cap Q||Q| = |P||Q| = pq$ as $|P \cap Q| \mid |P|$ and $|Q|$ by (C) implies $|P \cap Q| = 1$. Since $|G| = pq$ and $PQ \subseteq G$, $G = PQ$. Since $G = PQ$, $P \lhd G$, $Q \lhd G$, $P \cap Q = \{e\}$, $G = P \times Q$. Since both P and Q are of prime order, they are cyclic. Thus $G = P \times Q \approx \boldsymbol{Z}_p \oplus \boldsymbol{Z}_q \approx \boldsymbol{Z}_{pq}$, by (E). Hence G is cyclic. ■

   (c) If Q is not a normal subgroup, then $p \equiv 1$ (mod q) and $U(p)$ has a subgroup of order q.

   Soln. If Q is not normal, $1 < |G : N(Q)| \equiv 1$ (mod q). By (C), $|G : N(Q)|$ is a divisor of pq. Hence $|G : N(Q)| = p$ and $q \mid p - 1$. Since p is a prime, $|U(p)| = \varphi(p) = p - 1$ and $U(p)$ has a subgroup of order q by (E). ■

   (d) Let $p = 11$ and $q = 5$. <u>Find</u> an element $r \in U(11)$ of order 5. Let $N = \langle a \rangle$ be a cyclic group of order 11 and $H = \{1, r, r^2, r^3, r^4\}$. Set $G = N \times H$. Then G is a non-Abelian group of order 55 with respect to the following binary operation:

   $$G \times G \to G\ ((a^h, r^i)(a^j, r^k) \mapsto (a^{h+r^i j}, r^{i+k})),\ \text{where } 0 \le h, j \le 10,\ 0 \le i, k \le 4.$$

Soln. $|U(11)| = 10$. 2^2, $2^5 \not\equiv 1 \pmod{11}$, $|2| = 10$ in $U(11)$. Thus $r \in \{3, 4, 5, 9\}$ and $H = \{1, 4, 5, 9, 3\}$. Since

$$((a^h, r^i)(a^j, r^k))(a^\ell, r^m) = (a^{h+r^i j}, r^{i+k})(a^\ell, r^m) = (a^{h+r^i j+r^{i+k}\ell}, r^{i+k+m}) \text{ and}$$

$$(a^h, r^i)((a^j, r^k)(a^\ell, r^m)) = (a^h, r^i)(a^{j+r^k\ell}, r^{k+m}) = (a^{h+r^i(j+r^k\ell)}, r^{i+k+m}),$$

the operation is associative. $(e, 1)$ is the identity element and $(a^h, r^i)^{-1} = (a^{-r^{-i}h}, r^{-i})$. ■

Let N be a group and $H \leq \mathrm{Aut}(N)$. Then $G = N \times H$ becomes a group with respect to the following binary operation.

$$G \times G \to G \ ((x, \sigma) \cdot (y, \tau) \mapsto (x\sigma(y), \sigma\tau)).$$

In 5 (d), we apply 4 (d) and $H = \langle r \rangle \leq U(p) = \mathrm{Aut}(P)$. Moreover, when $y = a^j$ and $\sigma = r^i$, $\sigma(y) = \sigma(a^j) = a^{r^i j}$. Therefore when $x = a^h$, $x\sigma(y) = a^h a^{r^i j} = a^{h+r^i j}$. This is called a semi-direct product of N and H.