Algebra I: Final 2011

June 24, 2011

ID#: **Name:**

Quote the following when necessary.

Subgroup H of a group G:

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

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 $g^n = e$.

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

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 $(gH)(g'H) = gg'H$.

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

Kernel: If $\phi : G \to \overline{G}$ is a group homomorphism, $\mathrm{Ker}(\phi) = \{x \in G \mid \phi(x) = e_{\overline{G}}\}$, where $e_{\overline{G}}$ is the identity element of $\overline{G}$.

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 $N(P) = \{x \in G \mid xPx^{-1} = P\}$.

1. Let a be an element of order n. If k is an integer such that $\gcd\{k, n\} = 1$, then $C(a) = C(a^k)$. Here for $x \in G$, $C(x) = \{g \in G \mid gxg^{-1} = x\}$. You may use the fact that there exist $s, t \in \boldsymbol{Z}$ such that $ks + nt = 1$. (10 pts)

ID#: **Name:**

2. Let H and K be subgroups of a group G. Show the following. (25 pts)

   (a) For $x \in G$, $xH = H$ if and only if $x \in H$.

   (b) $H = HH = H^{-1}$.

   (c) HK is a subgroup of G if and only if $HK = KH$.

   (d) If $xhx^{-1} \in H$ for all $x \in G$ and $h \in H$, then H is a normal subgroup of G.

ID#: **Name:**

3. Let $\boldsymbol{R}^*$ denote the multiplicative group of nonzero real numbers and let

$$G = \left\{ \begin{bmatrix} a & c \\ 0 & b \end{bmatrix} \;\middle|\; a, b, c \in \boldsymbol{R} \text{ and } ab \neq 0 \right\}, \; H = \boldsymbol{R}^* \oplus \boldsymbol{R}^* = \{(x, y) \mid x, y \in \boldsymbol{R} - \{0\}\}.$$

Let

$$\phi : G \to H \quad \left(\begin{bmatrix} a & c \\ 0 & b \end{bmatrix} \mapsto (a, b) \right).$$

Show the following. (25 pts)

(a) G is a subgroup of $\mathrm{GL}(2, \boldsymbol{R})$, the multiplicative group consisting of invertible 2×2 real matrices. You may assume that $\mathrm{GL}(2, \boldsymbol{R})$ is a group.

(b) ϕ is an onto group homomorphism.

(c) $\mathrm{Ker}(\phi) \approx \boldsymbol{R}$, where $\boldsymbol{R}$ denote the additive group of real numbers.

(d) Suppose N is a subgroup of G containing $\mathrm{Ker}(\phi)$. Then N is a normal subgroup of G and G/N is Abelian.

ID#: **Name:**

4. Answer the following questions on Abelian groups of order $72 = 2^3 \cdot 3^2$. (20 pts)

   (a) Using the Fundamental Theorem of Finite Abelian Groups and list all non-isomorphic Abelian groups of order 72 and give a brief explanation.

   (b) List all Abelian groups of order 72 in your list above that have exactly three elements of order 2. Give your reason.

   (c) Determine whether or not $U(91) \approx U(152)$. Give your reason.

ID#: **Name:**

5. Let G be a non-Abelian group of order 21, P a Sylow 7-subgroup and Q a Sylow 3-subgroup of G. (20 pts)

   (a) Show that P and Q are cyclic.

   (b) Show that P is a normal subgroup of G.

   (c) Show that Q is not a normal subgroup of G.

   (d) Let $P = \langle x \rangle$ and $Q = \langle y \rangle$. Show that $yxy^{-1} \in \{x^2, x^4\}$.

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

Algebra I: Solutions to Final 2011

June 24, 2011

1. Let a be an element of order n. If k is an integer such that $\gcd\{k, n\} = 1$, then $C(a) = C(a^k)$. Here for $x \in G$, $C(x) = \{g \in G \mid gxg^{-1} = x\}$. You may use the fact that there exist $s, t \in \boldsymbol{Z}$ such that $ks + nt = 1$. (10 pts)

   Solution. First we prove the following claim.

   Claim: For every integer i, $C(x) \subset C(x^i)$.

   Proof. Let $g \in C(x)$. Then $gxg^{-1} = x$. Hence $x^i = (gxg^{-1})^i = gx^ig^{-1}$. Thus $g \in C(x^i)$. ■

   Let $s, t \in \boldsymbol{Z}$ be as above. By the claim above, $C(a) \subset C(a^k)$. On the other hand, $a = a^{ks+nt} = a^{ks}a^{nt} = (a^k)^s$. Therefor $C(a^k) \subset C((a^k)^s) = C(a)$. Therefore $C(a) = C(a^k)$ whenever $\gcd\{k, n\} = 1$. ■

2. Let H and K be subgroups of a group G. Show the following. (25 pts)

   (a) For $x \in G$, $xH = H$ if and only if $x \in H$.

   (b) $H = HH = H^{-1}$.

   (c) HK is a subgroup of G if and only if $HK = KH$.

   (d) If $xhx^{-1} \in H$ for all $x \in G$ and $h \in H$, then H is a normal subgroup of G.

   Solution. (a) Suppose $xH = H$. Since H is a subgroup, $e \in H$. Hence $x = xe \in xH = H$. Conversely, if $x \in H$, then since H is a subgroup,

   $$xH \subset HH \subset H = eH = xx^{-1}H \subset xHH \subset xH.$$

   Therefore $xH = H$. ■

   (b) Since H is a subgroup,

   $$H = eH \subset HH \subset H, \quad H^{-1} \subset H = (H^{-1})^{-1} \subset H^{-1}.$$

   Therefore $H = HH = H^{-1}$. ■

   (c) Suppose H is a subgroup of G. Then by (b)

   $$HK = (HK)^{-1} = K^{-1}H^{-1} = KH.$$

   Conversely suppose $HK = KH$. Then

   $$HKHK = HHKK = HK, \text{ and } (HK)^{-1} = K^{-1}H^{-1} = KH = HK.$$

   Therefore HK is a subgroup of G. ■

   (d) By assumption, $xHx^{-1} \subset H$ for every $x \in G$. Since $x^{-1} \in G$, $x^{-1}Hx = x^{-1}H(x^{-1})^{-1} \subset H$. Therefore

   $$xHx^{-1} \subset H = x(x^{-1}Hx)x^{-1} \subset xHx^{-1}.$$

   Thus $xHx^{-1} = H$ for evert $x \in G$ and H is a normal subgroup of G. ■

3. Let $\boldsymbol{R}^*$ denote the multiplicative group of nonzero real numbers and let

$$G = \left\{ \begin{bmatrix} a & c \\ 0 & b \end{bmatrix} \,\middle|\, a, b, c \in \boldsymbol{R} \text{ and } ab \neq 0 \right\}, \; H = \boldsymbol{R}^* \oplus \boldsymbol{R}^* = \{(x, y) \mid x, y \in \boldsymbol{R} - \{0\}\}.$$

Let

$$\phi : G \to H \quad \left(\begin{bmatrix} a & c \\ 0 & b \end{bmatrix} \mapsto (a, b) \right).$$

Show the following. (25 pts)

(a) G is a subgroup of $\mathrm{GL}(2, \boldsymbol{R})$, the multiplicative group consisting of invertible 2×2 real matrices. You may assume that $\mathrm{GL}(2, \boldsymbol{R})$ is a group.

(b) ϕ is an onto group homomorphism.

(c) $\mathrm{Ker}(\phi) \approx \boldsymbol{R}$, where $\boldsymbol{R}$ denote the additive group of real numbers.

(d) Suppose N is a subgroup of G containing $\mathrm{Ker}(\phi)$. Then N is a normal subgroup of G and G/N is Abelian.

Solution. (a) We show G is a subgroup of $\mathrm{GL}(2, \boldsymbol{R})$. Since

$$M^{-1} = \begin{bmatrix} a & c \\ 0 & b \end{bmatrix}^{-1} = \frac{1}{ab} \begin{bmatrix} b & -c \\ 0 & a \end{bmatrix}, \text{ and } MM' = \begin{bmatrix} a & c \\ 0 & b \end{bmatrix} \begin{bmatrix} a' & c' \\ 0 & b' \end{bmatrix} = \begin{bmatrix} aa' & ac' + cb' \\ 0 & bb' \end{bmatrix},$$

For $M, M' \in G$, $M^{-1} \in G$ and $MM' \in G$. Therefore G is a subgroup of $\mathrm{GL}(2, \boldsymbol{R})$. ■

(b) Using the computation above,

$$\phi(M)\phi(M') = (a, b)(a', b') = (aa', bb'), \text{ and } \phi(MM') = (aa', bb').$$

Therefore $\phi(MM') = \phi(M)\phi(M')$ and ϕ is a group homomorphism from G to H. For $(a, b) \in H$,

$$M = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \in G \text{ and } \phi(M) = (a, b).$$

Hence ϕ is onto. ■

(c) First we determine $\mathrm{Ker}(\phi)$. Since $e_H = (1, 1)$,

$$\mathrm{Ker}(\phi) = \left\{ \begin{bmatrix} 1 & c \\ 0 & 1 \end{bmatrix} \,\middle|\, c \in \boldsymbol{R} \right\}.$$

Let

$$\psi : \mathrm{Ker}(\phi) \to \boldsymbol{R} \quad \left(\begin{bmatrix} 1 & c \\ 0 & 1 \end{bmatrix} \mapsto c \right).$$

Since

$$\psi\left(\begin{bmatrix} 1 & c \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & c' \\ 0 & 1 \end{bmatrix} \right) = \psi\left(\begin{bmatrix} 1 & c + c' \\ 0 & 1 \end{bmatrix} \right) = c + c' = \psi\left(\begin{bmatrix} 1 & c \\ 0 & 1 \end{bmatrix} \right) + \psi\left(\begin{bmatrix} 1 & c' \\ 0 & 1 \end{bmatrix} \right),$$

ψ is a group homomorphism. It is clearly a bijection by definition. Therefore ψ is an isomorphism and $\mathrm{Ker}(\psi) \approx \boldsymbol{R}$.

(d) Since H is Abelian and $\phi(N)$ is a subgroup of H, $\phi(N)$ is a normal subgroup of H. Since ϕ is onto and N contains the kernel of ϕ, $\phi^{-1}(\phi(N)) = N$. (Clearly $\phi^{-1}(\phi(N)) \supset N$. For $M \in \phi^{-1}(\phi(N))$, there exists $M' \in N$ such that $\phi(M) = \phi(M')$ as $\phi(M) \in \phi(N)$. Therefore $MM'^{-1} \in \mathrm{Ker}(\phi)$ and $M \in \mathrm{Ker}(\phi)M' \in N$. Thus $\phi^{-1}(\phi(N)) \subset N$.) Let

$$\Phi : G \to H/\phi(N) \quad (M \mapsto \phi(M)\phi(N)).$$

Then $\mathrm{Ker}(\Phi) = \phi^{-1}(\phi(N)) = N$, and $G/N \approx H/\phi(N)$. Since H is Abelian, $H/\phi(N)$ is Abelian. Therefore G/N is Abelian. ■

4. Answer the following questions on Abelian groups of order $72 = 2^3 \cdot 3^2$. (20 pts)

   (a) Using the Fundamental Theorem of Finite Abelian Groups and list all non-isomorphic Abelian groups of order 72 and give a brief explanation.

   (b) List all Abelian groups of order 72 in your list above that have exactly three elements of order 2. Give your reason.

   (c) Determine whether or not $U(91) \approx U(152)$. Give your reason.

Solution. (a) By the Fundamental Theorem of Finite Abelian Group, every Abelian group of order 72 is isomorphic to an external direct product of cyclic groups $\boldsymbol{Z}_{e_1}, \boldsymbol{Z}_{e_2}, \ldots, \boldsymbol{Z}_{e_r}$ such that $e_i \mid e_{i+1}$ for $i = 1, 2, \ldots, r-1$, and $(e_1, e_2, \ldots, e_r)$ is uniquely determined. Since $72 = e_1 e_2 \cdots e_r$, the only possibilities of the sequences are (72), $(2, 36)$, $(2, 2, 18)$, $(3, 24)$, $(6, 12)$, and $(2, 6, 6)$. Therefore every finite Abelian group of order 72 is isomorphic one of the following groups.

$$\boldsymbol{Z}_{72},\ \boldsymbol{Z}_2 \oplus \boldsymbol{Z}_{36},\ \boldsymbol{Z}_2 \oplus \boldsymbol{Z}_2 \oplus \boldsymbol{Z}_{18},\ \boldsymbol{Z}_3 \oplus \boldsymbol{Z}_{24},\ \boldsymbol{Z}_6 \oplus \boldsymbol{Z}_{12},\ \text{or}\ \boldsymbol{Z}_2 \oplus \boldsymbol{Z}_6 \oplus \boldsymbol{Z}_6$$

(b) The order of element $(a_1, a_2, \ldots, a_r) \in \boldsymbol{Z}_{e_1} \oplus \boldsymbol{Z}_{e_2} \oplus \cdots \oplus \boldsymbol{Z}_{e_r}$ is $\mathrm{lcm}(|a_1|, |a_2|, \ldots, |a_r|)$. Therefore the groups in the list have the following number of elements of order 2 respectively, $1, 3, 7, 1, 3, 7$. Therefore groups satisfying the condition are

$$\boldsymbol{Z}_2 \oplus \boldsymbol{Z}_{36},\ \text{and}\ \boldsymbol{Z}_6 \oplus \boldsymbol{Z}_{12}.$$

(c) $91 = 7 \cdot 13$ and $152 = 8 \cdot 19$. Therefore

$$U(91) \approx U(7) \oplus U(13) \text{ and } U(152) \approx U(8) \times U(19).$$

Since $U(7), U(13), U(19)$ has exactly one element of order 2 and $U(8)$ has three elements of order 2, $U(19)$ has three elements of order 2 and $U(152)$ has seven elements of order 2. Thus these groups are not isomorphic. ■

5. Let G be a non-Abelian group of order 21, P a Sylow 7-subgroup and Q a Sylow 3-subgroup of G. (20 pts)

   (a) Show that P and Q are cyclic.

   (b) Show that P is a normal subgroup of G.

   (c) Show that Q is not a normal subgroup of G.

   (d) Let $P = \langle x \rangle$ and $Q = \langle y \rangle$. Show that $yxy^{-1} \in \{x^2, x^4\}$.

Solution. (a) Every groups of prime order are cyclic. (Let $|G| = p$, where p is a prime. Let $e \neq x \in G$. Then $H = \langle x \rangle$ is a subgroup of G of order at least 2. By Lagrange's Theorem, $|H| = |G|$ and $H = G$. Hence G is cyclic.) Since $|P| = 7$ and $|Q| = 3$, both P and Q are cyclic as 7 and 3 are prime. ■

(b) By Sylow's Theorem, $|G : N(P)| = |\mathrm{Syl}_7(G)| \equiv 1 \pmod 7$. Since $|G : N(P)|$ is a divisor of $|G|$ by Lagrange's Theorem, we have $|G : N(P)| = 1$ and $G = N(P)$. By the definition of $N(P)$, $G = N(P)$ means P is a normal subgroup. ■

(c) By way of contradiction, assume that Q is a normal subgroup. Then $|P \cap Q|$ is a divisor of $|P|$ and $|Q|$ and $P \cap Q = \{e\}$. Now PQ is a subgroup of G of order divisible by 7 and 3, we have $G = PQ$ and $G = P \times Q$. By (a), both P and Q are cyclic, so Abelian, G is Abelian. This contradicts our assumption. Thus Q is not normal in G. ■

(d) Since P is normal in G, $yxy^{-1} \in P = \langle x \rangle$. Suppose $yxy^{-1} = x^i$. Then

$$x = yyyxy^{-1}y^{-1}y^{-1} = yyx^iy^{-1}y^{-1} = yx^{i^2}y^{-1} = x^{i^3}.$$

Therefore $i^3 - 1 \equiv 0 \pmod 7$. Thus $yxy^{-1} \in \{x, x^2, x^4\}$. However $yxy^{-1} = x$ does not occur, as x and y are not commutative. ■