Math 31 – Final Exam Solutions

Due August 26, 2013 at 5:00 pm

Name: _____

Instructions: You may use your textbook (Saracino), the reserve text (Gallian), your notes from class (including the online lecture notes), and your old homework assignments. All other written materials are forbidden, as are any other electronic materials. You may not discuss the exam with anyone, and I will not give any assistance in solving the problems. You may ask me to clarify questions if necessary.

For any question labeled "show" or "prove," you should write a formal proof, using complete sentences and proper English.

Please hand this sheet in with your solutions. The exam is due on **Monday, August 26 at 5:00 pm**.

Honor statement:

I have neither given nor received any help on this exam, and I have not discussed the exam with anyone. I attest that all of the answers are my own work.

_____

Signature

Question	Points	Score
1	12	
2	8	
3	8	
4	16	
5	14	
6	16	
7	16	
8	10	
Total	100	

1. [12 points] For each of the following statements, either give an example which has the given property, or explain why no such example exists. You should give justification in either case, but a formal proof is not necessary.

(a) [3 points] Two abelian groups H and K such that $G = H \times K$ is nonabelian.

Solution. There is no example—the direct product of two abelian groups is always abelian. (You proved this on Homework 6, #7.)

(b) [3 points] A *nonabelian* group G and a normal subgroup $N \trianglelefteq G$ such that N and G/N are both cyclic groups.

Solution. The simplest example is D_3, but any dihedral group D_n would work. The rotation subgroup R is cyclic, and D_n/R has two elements, so it is cyclic as well.

(c) [3 points] An integral domain R and an ideal $I \subseteq R$ such that R/I contains zero divisors.

Solution. Let $R = \mathbb{Z}$ and let $I = 6\mathbb{Z}$. Then $\mathbb{Z}/6\mathbb{Z}$ contains zero divisors (for example, 2 and 3). You could also take any *composite* integer n in place of 6 here.

(d) [3 points] A ring R and a ring homomorphism $\varphi : \mathbb{Q} \to R$ such that $\ker \varphi = \mathbb{Z}$.

Solution. This is impossible. We know that the kernel of any ring homomorphism must be an ideal, but $\mathbb{Z}$ is not an ideal in $\mathbb{Q}$. (In fact, any ring homomorphism $\varphi : \mathbb{Q} \to R$ is either identically 0 or injective, since the only ideals of $\mathbb{Q}$ are $\{0\}$ and $\mathbb{Q}$.)

2. [8 points] Classify, up to isomorphism, all abelian groups of order 720.

Solution. Note that $720 = 2^4 \cdot 3^2 \cdot 5$, so there are 10 possible abelian groups of order 720: the abelian groups of order 2^4 are

$$\begin{aligned} &\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \\ &\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \\ &\mathbb{Z}_2 \times \mathbb{Z}_8 \\ &\mathbb{Z}_4 \times \mathbb{Z}_4 \\ &\mathbb{Z}_{16}, \end{aligned}$$

and the abelian groups of order 3^2 are just

$$\mathbb{Z}_3 \times \mathbb{Z}_3 \text{ and } \mathbb{Z}_9.$$

Therefore, the abelian groups of order 720 are:

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$$
$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$$
$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$$
$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5$$
$$\mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$$
$$\mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5$$
$$\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$$
$$\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5$$
$$\mathbb{Z}_{16} \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$$
$$\mathbb{Z}_{16} \times \mathbb{Z}_9 \times \mathbb{Z}_5$$

3. [8 points] Let G be a group, and let H be a subgroup of G with $[G : H] = 2$. Prove that $a^2 \in H$ for all $a \in G$.

Proof. Let $a \in G$. If $a \in H$, then we are done: H is a subgroup of G, so $a^2 \in H$ automatically. On the other hand, suppose that $a \in G - H$. Then $a^{-1} \in G - H$ as well: if a^{-1} belonged to H, then $(a^{-1})^{-1} = a \in H$ as well, since H is a subgroup. Since H has only two cosets, this means that $Ha = Ha^{-1}$. But this can occur only if

$$a(a^{-1})^{-1} \in H,$$

which means that $a^2 \in H$.

4. [16 points] Let $\tau \in S_n$, and write τ as a product of disjoint cycles (including 1-cycles):

$$\tau = \tau_1 \tau_2 \cdots \tau_m.$$

Let k_i be the length of τ_i for $1 \leq i \leq m$, and order the cycles so that $k_1 \leq k_2 \leq \cdots \leq k_m$. The m-tuple $(k_1, k_2, \ldots, k_m)$ is called the **cycle type** of τ. For example, the permutation

$$(1\ 3)(2\ 5\ 6)(7\ 8) = (4)(1\ 3)(7\ 8)(2\ 5\ 6)$$

in S_8 has cycle type $(1, 2, 2, 3)$.

(a) [8 points] Let $(x_1\ x_2\ \cdots\ x_k)$ be a k-cycle in S_n. Prove that for any $\sigma \in S_n$,

$$\sigma(x_1\ x_2\ \cdots\ x_k)\sigma^{-1} = (\sigma(x_1)\ \sigma(x_2)\ \cdots\ \sigma(x_k)).$$

Proof. Let $\sigma \in S_n$, and let $\tau = (x_1\ x_2\ \cdots\ x_k)$. Then for any $x \in \{1, 2, \ldots, n\}$, we have

$$\sigma\tau\sigma^{-1}(x) = \sigma(\tau(\sigma^{-1}(x))).$$

If $\sigma^{-1}(x) \notin \{x_1, x_2, \ldots, x_k\}$ (which is the same as saying that $x \notin \{\sigma(x_1), \sigma(x_2), \ldots, \sigma(x_k)\}$), then τ fixes $\sigma^{-1}(x)$, and we have

$$\sigma\tau\sigma^{-1}(x) = \sigma\sigma^{-1}(x) = x.$$

Therefore, we need only consider $x \in \{\sigma(x_1), \sigma(x_2), \ldots, \sigma(x_k)\}$. Then we have

$$\begin{aligned}
\sigma\tau\sigma^{-1}(\sigma(x_1)) &= \sigma\tau(x_1) = \sigma(x_2) \\
\sigma\tau\sigma^{-1}(\sigma(x_2)) &= \sigma\tau(x_2) = \sigma(x_3) \\
&\vdots \\
\sigma\tau\sigma^{-1}(\sigma(x_{k-1}) &= \sigma\tau(x_{k-1}) = \sigma(x_k) \\
\sigma\tau\sigma^{-1}(\sigma(x_k) &= \sigma\tau(x_k) = \sigma(x_1).
\end{aligned}$$

Therefore, we see that

$$\sigma\tau\sigma^{-1} = (\sigma(x_1)\ \sigma(x_2)\ \cdots\ \sigma(x_k)),$$

as desired.

(b) [8 points] Prove that for any $\sigma \in S_n$, $\sigma\tau\sigma^{-1}$ has the same cycle type as τ.

Proof. Fix $\tau \in S_n$, and suppose that τ has cycle type $(k_1, k_2, \ldots, k_m)$. That is, τ can be written in the form

$$\tau = \tau_1\tau_2\cdots\tau_m,$$

where the τ_i are disjoint cycles and τ_i has length k_i. Then for any $\sigma \in S_n$, we have

$$\begin{aligned}
\sigma\tau\sigma^{-1} &= \sigma(\tau_1\tau_2\cdots\tau_m)\sigma^{-1} \\
&= \sigma\tau_1\sigma^{-1}\sigma\tau_2\sigma^{-1}\sigma\cdots\sigma^{-1}\sigma\tau_m\sigma^{-1} \\
&= (\sigma\tau_1\sigma^{-1})(\sigma\tau_2\sigma^{-1})\cdots(\sigma\tau_m\sigma^{-1}).
\end{aligned}$$

Since each τ_i is a k_i-cycle, we know from part (a) that $\sigma_i = \sigma\tau_i\sigma^{-1}$ is also a k_i-cycle. It's also not hard to see that the σ_i must be disjoint, since the τ_i are. Therefore, $\sigma\tau\sigma^{-1}$ has cycle type $(k_1, k_2, \ldots, k_m)$, which is the same as that of τ.

5. [14 points] Let G be an abelian group. Define

$$\mathrm{Tor}(G) = \left\{ a \in G : a^m = e \text{ for some } m \in \mathbb{Z}^+ \right\}.$$

(Note that the integer m depends on a.) Equivalently, $\mathrm{Tor}(G)$ consists of all elements of G which have finite order. Then $\mathrm{Tor}(G)$ is a subgroup of G, called the **torsion subgroup**.

(a) [10 points] Show that the quotient group $G/\mathrm{Tor}(G)$ contains no elements of finite order except for the identity element.

Proof. Let $H = \mathrm{Tor}(G)$, and suppose that Ha has finite order in G/H. That is,

$$(Ha)^m = He$$

for some $m \in \mathbb{Z}$. That is, $Ha^m = He$, which means that $a^m \in H$. But H is the torsion subgroup, so a^m has finite order, say n. Then

$$(a^m)^n = a^{mn} = e,$$

so a has finite order. Therefore, a was in $H = \mathrm{Tor}(G)$ to begin with, so $Ha = He$. Therefore, the only element of finite order in $G/\mathrm{Tor}(G)$ is the coset He, which is simply the identity element.

(b) [4 points] Let $G = \mathbb{Z} \times \mathbb{Z}_5$. Find $\mathrm{Tor}(G)$, and verify that $G/\mathrm{Tor}(G) \cong \mathbb{Z}$.

Proof. A pair $(a, b) \in G$ belongs to $\mathrm{Tor}(G)$ if there is an integer m such that

$$m \cdot (a, b) = (m \cdot a, m \cdot b) = (0, 0).$$

This means that $m \cdot a = 0$ and $m \cdot b = 0$. The only element of $\mathbb{Z}$ with finite order is 0, so we need $a = 0$. Now if $a = 0$ and $b \in \mathbb{Z}_5$ is any element of $\mathbb{Z}_5$, then we can find an m such that $m \cdot (a, b) = 0$. (Just take $m = o(b)$.) Therefore,

$$\mathrm{Tor}(G) = \{(0, b) \in G : b \in \mathbb{Z}_5\} \cong \mathbb{Z}_5.$$

Now define $\varphi : G \to \mathbb{Z}$ by $\varphi(a, b) = a$. Then it is easy to see that $\ker \varphi = \mathrm{Tor}(G)$, so the Fundamental Homomorphism Theorem guarantees that $G/\mathrm{Tor}(G) \cong \mathbb{Z}$.

6. [16 points] Let G be a group, and define

$$D = \{(a, a) \in G \times G : a \in G\}.$$

In general, D is a subgroup of $G \times G$ and $D \cong G$. (You may assume these facts throughout this problem.)

(a) [6 points] Prove that D is a normal subgroup of $G \times G$ if and only if G is abelian.

Proof. Suppose first that G is abelian. Then we have seen before that $G \times G$ is also abelian, and that any subgroup of an abelian group is normal, so D is normal in $G \times G$.

On the other hand, suppose that D is normal in $G \times G$. Then given $a, b \in G$, we have

$$(b, e)(a, a)(b, e)^{-1} = (bab^{-1}, a) \in D.$$

This means that $bab^{-1} = a$, or $ba = ab$. Since $a, b \in G$ are arbitrary, it follows that G is abelian.

(b) [10 points] Suppose that G is abelian. Prove that $(G \times G)/D \cong G$.

Proof. We will invoke the Fundamental Homomorphism Theorem. Therefore, we need an epimorphism $\varphi : G \times G \to G$ such that $\ker \varphi = D$. We'll define φ by

$$\varphi(a, b) = ab^{-1}.$$

To see that this is a homomorphism, let $(a, b), (c, d) \in G \times G$. Then (since G is abelian),

$$\varphi((a, b)(c, d)) = \varphi(ac, bd) = ac(bd)^{-1} = acd^{-1}b^{-1} = (ab^{-1})(cd^{-1}) = \varphi(a, b)\varphi(c, d).$$

Furthermore, φ is onto: given $a \in G$, observe that

$$\varphi(a, e) = ae^{-1} = a.$$

Finally, we check that $\ker \varphi = D$. If $(a, a) \in D$, then we certainly have

$$\varphi(a, a) = aa^{-1} = e,$$

so $(a, a) \in \ker \varphi$. On the other hand, if $\varphi(a, b) = e$, then $ab^{-1} = e$, so $a = b$. Therefore, $(a, b) \in D$, and $\ker \varphi = D$. The Fundamental Homomorphism Theorem then implies that

$$(G \times G)/D = (G \times G)/\ker \varphi \cong G.$$

7. [16 points] Let $R = \mathrm{M}_2(\mathbb{R})$, the ring of all 2-by-2 matrices with real coefficients.

(a) [8 points] Define a subset $S \subseteq R$ by

$$S = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R} \right\}.$$

Verify that S is a subring of R, and that $S^\times = S - \{0\}$.

Proof. We need to check that S is a subgroup of R under addition, and that it is closed under multiplication. Observe that

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ -b-d & a+c \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix}$$

so S is closed under addition. Similarly,

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -bc-ad & -bd+ac \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix}$$

so S is closed under multiplication. The zero matrix clearly belongs to S, and S is closed under additive inverses:

$$-\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} -a & -b \\ b & -a \end{pmatrix} \in S.$$

Therefore, S is a subring of R. To compute $S^\times$, we need to determine which elements of S have multiplicative inverses. The elements of S are matrices, so we can determine which matrices are invertible by considering the determinant. Given a matrix $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ in S, we have

$$\det \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a^2 + b^2,$$

which equals 0 if and only if $a = 0$ and $b = 0$. Therefore, if $A \in S$, $\det A = 0$ if and only if $A = 0$, and it follows that $S^\times = S - \{0\}$.

(b) [8 points] Define $\varphi : \mathbb{C} \to \mathrm{M}_2(\mathbb{R})$ by

$$\varphi(a + bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Prove that φ is a ring isomorphism of $\mathbb{C}$ onto the subring S defined in part (a).

Proof. We first check that φ is a ring homomorphism. Given two complex numbers $a+bi$ and $c+di$, we have

$$\varphi((a+bi)+(c+di)) = \varphi((a+c)+(b+d)i) = \begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix}$$

while

$$\varphi(a+bi)+\varphi(c+di) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix}.$$

Therefore, φ preserves addition. Similarly,

$$\varphi((a+bi)(c+di)) = \varphi((ac-bd)+(ad+bc)i) = \begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix},$$

while

$$\varphi(a+bi)\varphi(c+di) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix}.$$

Therefore, φ is a ring homomorphism. It is easy to see that φ is onto, and it is one-to-one since $\varphi(a+bi)=0$ implies that $a=0$ and $b=0$. Thus $\ker\varphi = \{0\}$, and φ is an isomorphism.

8. [10 points] Let R be a commutative ring, and fix $a \in R$. Define the **annihilator** of a to be the set

$$\mathrm{Ann}(a) = \{x \in R : xa = 0\}.$$

(a) [8 points] Prove that $\mathrm{Ann}(a)$ is an ideal of R.

Proof. We need to check that $\mathrm{Ann}(a)$ is an additive subgroup of R and that it "absorbs" elements of R under multiplication. Suppose that $x, y \in \mathrm{Ann}(a)$. Then the distributive law implies

$$(x+y)a = xa + ya = 0 + 0 = 0,$$

so $x+y \in \mathrm{Ann}(a)$, and the annihilator is closed under addition. Also, $0 \cdot a = 0$, so $0 \in \mathrm{Ann}(a)$. Finally, if $x \in \mathrm{Ann}(a)$, then

$$(-x)a = -(xa) = -0 = 0,$$

so $-x \in \mathrm{Ann}(a)$ as well. Therefore, $\mathrm{Ann}(a)$ is a subgroup of R under addition.

Now let $x \in \mathrm{Ann}(a)$, and let $r \in R$. Then the associativity of multiplication implies that

$$(rx)a = r(xa) = r \cdot 0 = 0.$$

Since R is commutative, we also have

$$(xr)a = (rx)a = 0,$$

so $rx, xr \in \mathrm{Ann}(a)$. Therefore, $\mathrm{Ann}(a)$ is an ideal of R.

(b) [2 points] Find the annihilator of 8 in $\mathbb{Z}_{12}$.

Proof. We are looking for elements $x \in \mathbb{Z}_{12}$ with the property that $x \cdot_{12} 8 = 0$. This amounts to finding integers x such that $x \cdot 8$ is a multiple of 12. Certainly 0 works, and the others are 3, 6, and 9. Therefore,

$$\mathrm{Ann}(a) = \{0, 3, 6, 9\}.$$

Note that this is just the cyclic subgroup $\langle 3 \rangle$ generated by 3 in $\mathbb{Z}_{12}$. (It is also the principal ideal (3) generated by 3.)