Math 516 **Fall 2006** **Radford**

Solution to the Final Examination 12/17/06

Name (PRINT) ____

(1) *Return* this exam copy. (2) *Write* your solutions in your exam booklet. (3) *Show* your work. (4) There are *eight questions* on this exam. (5) Each question counts 25 points. (6) *You are expected to abide by the University's rules concerning academic honesty.*

---

1. (**25 points total**) Let $G = <a>$ be a cyclic group of order 55.

(a) (**5**) How many subgroups does G have?

Solution: 4 subgroups since there are 4 divisors of $55 = 5{\cdot}11$.

(b) (**5**) Find $|a^{-100}|$.

Solution: 11, since $|a^{-100}| = |a^{(-100,55)}| = |a^{(-100,5\cdot 11)}| = |a^5| = 55/5 = 11$.

(c) (**5**) Find the number of elements of orders $1, 5, 11$, respectively and find the number of generators of G.

Solution: $\varphi(1) = 1$, $\varphi(5) = 4$, $\varphi(11) = 10$, and $\varphi(55) = 55-(\varphi(1)+\varphi(5)+\varphi(11)) = 55-(1+4+10) = 40$.

(d) (**5**) Which of the elements in the list $a^{20}, a^{21}, \ldots, a^{30}$ are generators of G?

Solution: a^{21}, a^{23}, a^{24}, a^{26}, a^{27}, a^{28}, a^{29} as a^d generates G if and only if $(d, |G|) = 1$.

(e) (**5**) List the elements of $<a^{22}>$ in the form a^ℓ, where $0 \leq \ell < 55$.

Solution: $\{e, a^{11}, a^{22}, a^{33}, a^{44}\}$ as $<a^{22}> = <a^{(22,55)}> = <a^{11}>$.

2. (**25 points total**) Let $\mathrm{GL}_2(\mathbf{R})$ be the group of invertible $2{\times}2$ matrices with real coefficients under matrix multiplication and let

$$G = \{\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \mid ad \neq 0\}.$$

(a) (**14**) Show that $G \leq \mathrm{GL}_2(\mathbf{R})$.

Solution: $G \neq \emptyset$ as $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in G$. Suppose that $\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}, \begin{pmatrix} a' & 0 \\ c' & d' \end{pmatrix} \in G$. Then $ad, a'd' \neq 0$; hence $a^{-1}d^{-1}, aa'dd' \neq 0$. Thus $\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}\begin{pmatrix} a' & 0 \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' & 0 \\ ca' + dc' & dd' \end{pmatrix} \in G$ and $\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} a^{-1} & 0 \\ -ca^{-1}d^{-1} & d^{-1} \end{pmatrix} \in G$.

(b) (**11**) The subgroup $H \leq G$ of diagonal matrices (c = 0) acts on $A = \mathbf{R}^2$ by matrix multiplication. Find the H-orbits of A and find the stabilizer of $\begin{pmatrix} 0 \\ 5 \end{pmatrix}$.

Solution: $\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax \\ dy \end{pmatrix}$. Thus the orbits are

$$\{\begin{pmatrix} 0 \\ 0 \end{pmatrix}\}, \quad \{\begin{pmatrix} a \\ 0 \end{pmatrix} \mid a \neq 0\}, \quad \{\begin{pmatrix} 0 \\ d \end{pmatrix} \mid d \neq 0\}, \quad \{\begin{pmatrix} a \\ d \end{pmatrix} \mid a, d \neq 0\}$$

as these are orbits which partition A. The H-stabilizer of $\begin{pmatrix} 0 \\ 5 \end{pmatrix}$ is $\{\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \mid a \neq 0\}$.

3. (**25 points total**) Let p be a prime integer and G a finite-abelian group such that $a^p = e$ for all $a \in G$. Suppose $H \leq G$.

(a) (**15**) Assume $a \notin H$ and let $K = <a>$. Show that $HK \leq G$ and $|HK| = |H||K|$

Solution: Since G is commutative, $HK = KH$ and thus $HK \leq G$. Since $a^p = e \neq a$ it follows that $K = <a>$ has order p. Since $H \cap K \leq H, K$ by Lagrange's Theorem $|H \cap K|$ divides both $|H|$ and $|K| = p$. If $|H \cap K| = p$ then $a \in H \cap K = K$, contradiction. Therefore $|H \cap K| = 1$ and $|H||K| = |HK||H \cap K| = |HK|$.

(b) (**10**) Suppose that H is a maximal proper subgroup of G. Show that $|G{:}H| = p$.

Solution: Since H is proper, there is an $a \in G$ such that $a \notin H$. Let $K = <a>$. By part (a) $HK \leq G$ and $|HK| = |H||K| = |H|p$. Since H is maximal, $HK = G$. Thus $|G| = |HK| = |H|p$ which implies $|G{:}H| = p$.

4. (**25 points total**) Let G be a finite group of order $3{\cdot}5^2{\cdot}29$.

(a) (**10**) Show that G has a normal subgroup of order 29.

Solution: Let n_p be the number of Sylow-p subgroups of G. Then $n_{29} = 1 + 29k$ for some non-negative integer k, and n_{29} divides $3{\cdot}5^2{\cdot}29$, hence divides $3{\cdot}5^2 = 75$. As n_{29} is among $1, 30, 59, 88, \ldots$ necessarily $n_{29} = 1$. This is enough to establish the normality of a Sylow-29 subgroup N of G.

(b) (**15**) Show that G has a subgroup of index 15.

Solution: G has a Sylow-5 subgroup H. Thus H has order 25. Let $e = a \in H$ and consider $K = <a>$. Then $|K| = 5$ or $|K| = 25$. In the latter case K has an element of order 5 since 5 divides $|<a>|$. (Also by Cauchy's Theorem G has an element of order 5.)

Thus G has a subgroup L of order 5. By Lagrange's Theorem $L \cap N = (e)$. Since $N \trianglelefteq G$ it follows that $LN \leq G$. As $|N||L| = |NL||N \cap L| = |NL|$ we have $|G : NL| = |G|/|NL| = |G|/|N||L| = (3{\cdot}5^2{\cdot}29)/(5{\cdot}29) = 15$.

5. (**25 points total**) This question concerns the structure of finite abelian groups.

(a) (**5**) How many isomorphism types of abelian groups of order $2^3{\cdot}7^4{\cdot}11^2$ are there?

Solution: The partitions of 3 are $1+1+1, 2+1, 3$; the partitions of 4 are $1+1+1+1, 2+1+1, 2+2, 3+1, 4$, and the partitions of 2 are $1+1, 2$. Therefore there are $3{\cdot}5{\cdot}2 = 30$ isomorphism classes of abelian groups order $2^3{\cdot}7^4{\cdot}11^2$.

(b) (**20**) List the different isomorphism types of abelian groups of order $5^3{\cdot}7^2{\cdot}11$ as $\mathbf{Z}_{n_1} \times \cdots \times \mathbf{Z}_{n_s}$, where $1 < n_i$ for all $1 \leq i \leq s$, in *two* ways; first where $n_1, \ldots, n_s$ are prime powers, and secondly where $n_1 | n_2 | \cdots | n_s$. (In the second case you can express the n_i's as products.)

Solution: Counting partitions, there are $3{\cdot}2{\cdot}1 = 6$ types:

$\mathbf{Z}_5 \times \mathbf{Z}_5 \times \mathbf{Z}_5 \times \mathbf{Z}_7 \times \mathbf{Z}_7 \times \mathbf{Z}_{11} \simeq \mathbf{Z}_5 \times \mathbf{Z}_{5\cdot7} \times \mathbf{Z}_{5\cdot7\cdot11}$
$\mathbf{Z}_5 \times \mathbf{Z}_5 \times \mathbf{Z}_5 \times \mathbf{Z}_{7^2} \times \mathbf{Z}_{11} \simeq \mathbf{Z}_5 \times \mathbf{Z}_5 \times \mathbf{Z}_{5\cdot7^2\cdot11}$
$\mathbf{Z}_5 \times \mathbf{Z}_{5^2} \times \mathbf{Z}_7 \times \mathbf{Z}_7 \times \mathbf{Z}_{11} \simeq \mathbf{Z}_{5\cdot7} \times \mathbf{Z}_{5^2\cdot7\cdot11}$
$\mathbf{Z}_5 \times \mathbf{Z}_{5^2} \times \mathbf{Z}_{7^2} \times \mathbf{Z}_{11} \simeq \mathbf{Z}_5 \times \mathbf{Z}_{5^2\cdot7^2\cdot11}$
$\mathbf{Z}_{5^3} \times \mathbf{Z}_7 \times \mathbf{Z}_7 \times \mathbf{Z}_{11} \simeq \mathbf{Z}_7 \times \mathbf{Z}_{5^3\cdot7\cdot11}$
$\mathbf{Z}_{5^3} \cdot \mathbf{Z}_{7^2} \times \mathbf{Z}_{11} \simeq \mathbf{Z}_{5^3\cdot7^2\cdot11}$.

6. (**25 points total**) Let $R = \mathrm{M}_2(\mathbf{R})$ be the ring of 2×2 matrices with real coefficients, let $S = \{\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \mid a, c, d \in \mathbf{R}\}$.

(a) (**11**) Show that S is a subring of R.

Solution: $S \neq \emptyset$ the zero matrix belongs to S. Let $\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}, \begin{pmatrix} a' & 0 \\ c' & d' \end{pmatrix} \in S$. Since $\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} - \begin{pmatrix} a' & 0 \\ c' & d' \end{pmatrix} = \begin{pmatrix} a-a' & 0 \\ c-c' & d-d' \end{pmatrix} \in S$ and

$$\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}\begin{pmatrix} a' & 0 \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' & 0 \\ ca'+dc' & dd' \end{pmatrix} \in S$$

it follows that S is a subring of R.

(b) (**8**) Show that $f : S \longrightarrow \mathbf{R}$ defined by $f(\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}) = d$ is a ring homomorphism.

Solution:

$$\begin{aligned} & f(\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} + \begin{pmatrix} a' & 0 \\ c' & d' \end{pmatrix}) \\ = \ & f(\begin{pmatrix} a+a' & 0 \\ c+c' & d+d' \end{pmatrix}) \\ = \ & d + d' \\ = \ & f(\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}) + f(\begin{pmatrix} a' & 0 \\ c' & d' \end{pmatrix}) \end{aligned}$$

and

$$\begin{aligned} & f(\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \begin{pmatrix} a' & 0 \\ c' & d' \end{pmatrix}) \\ = \ & f(\begin{pmatrix} aa' & 0 \\ ca' + dc' & dd' \end{pmatrix}) \\ = \ & dd' \\ = \ & f(\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}) f(\begin{pmatrix} a' & 0 \\ c' & d' \end{pmatrix}) \end{aligned}$$

for all $\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}, \begin{pmatrix} a' & 0 \\ c' & d' \end{pmatrix} \in S$.

(c) (**6**) Show that the ideal $I = \mathrm{Ker} f$ is generated by a single element as a left ideal.

Solution: $\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix}$ for all $a, c, d \in \mathbf{R}$. As $\mathrm{Ker} f$ consists of the matrices just described, $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ is such a generator.

7. (**25 points total**) Decide whether or not each of the following polynomials

$$2X^2 + 9X + 3, \quad 2X^2 + 11X + 3, \quad 3X^2 + 9X + 9$$

is irreducible (a) over $\mathbf{Z}[X]$, (b) over $\mathbf{Q}[X]$. Justify your answers.

Solution: We consider each in turn.

($\mathbf{9}$) $2X^2 + 9X + 3 \in \mathbf{Z}[X]$ is irreducible by the Eisenstein Criterion with $p = 3$. Since it is primitive, $2X^2 + 9X + 3 \in \mathbf{Q}[X]$ is irreducible by the Gauss Lemma.

($\mathbf{8}$) $2X^2 + 9X + 3 \in \mathbf{Q}[X]$ is irreducible since it has no root in $\mathbf{Q}$. The possible roots are $\pm 1, \pm 1/2, \pm 3, \pm 3/2$. A root must be negative. Show that $-1, -3, -1/2, -3/2$ are not roots. Since $2X^2 + 9X + 3$ is also primitive $2X^2 + 9X + 3 \in \mathbf{Z}[X]$ is irreducible.

($\mathbf{8}$) $3X^2 + 9X + 9 = 3(x^2 + 3X + 3) \in \mathbf{Z}[X]$ is reducible since it is the product of non-zero non-units in $\mathbf{Z}[X]$. Now $X^2 + 3X + 3 \in \mathbf{Z}[X]$ is irreducible by the Eisenstein Criterion with $p = 3$. Thus, since 3 is a unit of $\mathbf{Q}$ and $X^2 + 3X + 3$ is primitive, it follows that $3X^2 + 9X + 9 = 3(X^2 + 3X + 3) \in \mathbf{Q}[X]$ is irreducible by the Gauss Lemma.

8. (**25 points total**) Let R be a ring, let M and M' be left R-modules, and let $\mathrm{Tor}(M)$ be the set of all elements $m \in M$ such that $r{\cdot}m = 0$ for some non-zero $r \in R$.

(a) (**5**) Let $f : M \longrightarrow M'$ be a map of left R-modules. Show that $f(\mathrm{Tor}(M)) \subseteq \mathrm{Tor}(M')$.

Solution: Let $m \in \mathrm{Tor}(M)$. Then $r{\cdot}m = 0$ for some non-zero $r \in R$. Since $r{\cdot}f(m) = f(r{\cdot}m) = f(0) = 0$, by definition $f(m) \in \mathrm{Tor}(M)$.

Now suppose that R is an integral domain.

(b) (**10**) Show that $\mathrm{Tor}(M)$ is a submodule of M.

Solution: First of all $\mathrm{Tor}(M) \neq \emptyset$ since $0 = 1{\cdot}0$ implies $0 \in \mathrm{Tor}(M)$. Suppose $m, n \in \mathrm{Tor}(M)$. Then $r{\cdot}m = 0 = s{\cdot}n$ for some non-zero $r, s \in R$. Since R is an integral domain $rs \neq 0$ and also R is a commutative with unity. Let $r' \in R$. Then the calculation

$$(rs){\cdot}(m + r'{\cdot}n) = (sr){\cdot}m + (rr's){\cdot}n = s{\cdot}(r{\cdot}m) + (rr'){\cdot}(s{\cdot}n) = s{\cdot}0 + (rr'){\cdot}0 = 0$$

shows that $m + r'{\cdot}n \in \mathrm{Tor}(M)$. Therefore $\mathrm{Tor}(M)$ is an R-submodule of M.

(c) (**10**) Show that $\mathrm{Tor}(M{\times}M') = \mathrm{Tor}(M){\times}\mathrm{Tor}(M')$.

Solution: Let $(m, m') \in \mathrm{Tor}(M{\times}M')$. Then there is a non-zero $r \in R$ such that $0 = r{\cdot}(m, m') = (r{\cdot}m, r{\cdot}m')$, or equivalently $r{\cdot}m = 0 = r{\cdot}m'$. Therefore $(m, m') \in \mathrm{Tor}(M){\times}\mathrm{Tor}(M')$. We have shown $\mathrm{Tor}(M{\times}M') \subseteq \mathrm{Tor}(M){\times}\mathrm{Tor}(M')$.

Conversely, suppose $(m, m') \in \mathrm{Tor}(M){\times}\mathrm{Tor}(M')$. Then there are non-zero $r, r' \in R$ such that $r{\cdot}m = 0 = r'{\cdot}m'$. Since R is an integral domain $rr' \neq 0$. Since

$$\begin{aligned}(rr'){\cdot}(m, m') &= ((rr'){\cdot}m, (rr'){\cdot}m') \\ &= ((r'r){\cdot}m, (rr'){\cdot}m') \\ &= (r'{\cdot}(r{\cdot}m), r{\cdot}(r'{\cdot}m')) \\ &= (r'{\cdot}0, r{\cdot}0) = (0, 0)\end{aligned}$$

it follows that $\mathrm{Tor}(M){\times}\mathrm{Tor}(M') \subseteq \mathrm{Tor}(M{\times}M')$.