Mathematics 351 – Abstract Algebra 1
Solutions for Final Examination
December 12, 2007

I. *Terminology*

A) (5) What does it mean to say that R is a *ring with identity*?

Solution: R is a ring with identity if there is a *multiplicative identity* $1 \in R$ – an element 1 such that $a \cdot 1 = a = 1 \cdot a$ for all $a \in R$.

B) (5) What does it mean to say that $a \in F$ is a *root* of $f(x) \in F[x]$?

Solution: The element $a \in F$ is a root of $f(x) \in F[x]$ if $f(a) = 0_F$.

C) (5) What does it mean to say that $f(x) \in F[x]$ is *irreducible*?

Solution: The polynomial $f(x)$ is irreducible in $F[x]$ if in every factorization $f(x) = g(x)h(x)$ in $F[x]$, one of $g(x), h(x)$ is a unit in $F[x]$ (a nonzero constant), and the other is an associate of $f(x)$.

D) (5) What does it mean to say that a subset I of a ring R is an *ideal* in R?

Solution: A nonempty subset I of a ring R is an ideal if it is a subring of R which has the property that $a \cdot r, r \cdot a \in I$ whenever $a \in I$ and $r \in R$ (I "absorbs all products with elements of I).

E) (5) What does it mean to say that a permutation $\sigma \in S_n$ is *even*?

Solution: The permutation σ is even if it is the product of an even number of transpositions (or equivalently if the determinant of the associated permutation matrix is $+1$.)

II.

A) (15) State and prove the Eisenstein Irreducibility Criterion in $\mathbb{Q}[x]$.

Solution: The statement is: Let $f(x) = a_n x^n + \cdots + a_1 x + a_0$ be a nonconstant polynomial in $\mathbb{Z}[x]$. Assume there is some prime $p \in \mathbb{Z}$ such that $p \not| a_n$, $p | a_{n-1}, \ldots, p | a_0$, but $p^2 \not| a_0$. Then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

- Proof: Arguing by contradiction, suppose $f(x) = g(x)h(x)$ where $g(x)$ and $h(x)$ both have positive degree. By Theorem 4.22, we can assume that $g(x), h(x) \in \mathbb{Z}[x]$ as well so write:

$$\begin{aligned} f(x) &= a_n x^n + \cdots + a_1 x + a_0 \\ &= (b_k x^k + \cdots + b_1 x + b_0)(c_\ell x^\ell + \cdots + c_1 x + c_0) \end{aligned}$$

for some $k, \ell \geq 1$. By hypothesis $p|a_0$ so $p|(b_0 c_0)$. However $p^2 \not| \, a_0$, so by renaming the polynomials $g(x), h(x)$ if necessary we may assume $p|b_0$ but $p \not| c_0$. Now look at the coefficient of x: $a_1 = b_0 c_1 + b_1 c_0$. We know $p|a_1$ and $p|b_0$, so $p|(b_1 c_0)$ as well. Since $p \not| c_0$, this implies that $p|b_1$ as well. We continue in the same way to show that $p|b_0, b_1, \ldots, b_k$. (Note that the process we started here will continue until the coefficient $a_k = b_0 c_k + b_1 c_{k-1} + \cdots + b_k c_0$ since $k < n$.) But now notice that $p|b_k$ implies $p|(b_k c_\ell)$, so $p|a_n$. This is a contradiction to the hypothesis that p does not divide the leading coefficient of $f(x)$, a_n. Hence $f(x)$ must be irreducible in $\mathbb{Q}[x]$.

B) (10) Use the Eisenstein criterion to show that there are irreducible polynomials of every degree ≥ 1 in $\mathbb{Q}[x]$.

Solution: We just need to "cook up" polynomials of each degree satisfying the hypotheses in the Eisenstein Criterion. One such way, using the prime $p = 2$: For all degrees $n \geq 1$, take

$$f(x) = x^n + 2.$$

These are all irreducible since all the conditions for Eisenstein are met.

III.

A) (10) Show that $a \in F$ is a root of $f(x) \in F[x]$ if and only if $(x - a)|f(x)$ in $F[x]$.

Solution: If $(x - a)|f(x)$, then $f(x) = q(x)(x - a)$ for some $q(x) \in F[x]$. Hence $f(a) = q(a)(a - a) = 0$. This shows a is a root of $f(x)$. Conversely, assume that $x = a$ is a root of $f(x)$ and use the division algorithm to divide $x - a$ into $f(x)$ and write $f(x) = q(x)(x - a) + r$. Since $deg(x - a) = 1$, $r \in F$ is a constant. However, if a is a root of $f(x)$, then $0 = f(a) = q(a)(a - a) + r = 0 + r$. Hence $r = 0$, so $x - a$ divides $f(x)$.

B) (10) Express $f(x) = x^4 - 16$ as a product of irreducible polynomials in $\mathbb{Q}[x]$, in $\mathbb{R}[x]$, and finally in $\mathbb{C}[x]$.

Solution:

- In $\mathbb{Q}[x]$: $x^4 - 16 = (x^2 - 4)(x^2 + 4) = (x - 2)(x + 2)(x^2 + 4)$.
- In $\mathbb{R}[x]$: $x^4 - 16 = (x^2 - 4)(x^2 + 4) = (x - 2)(x + 2)(x^2 + 4)$ (same)
- In $\mathbb{C}[x]$: $x^4 - 16 = (x - 2)(x + 2)(x - 2i)(x + 2i)$.

We know that x^2+4 is irreducible over $\mathbb{Q}[x]$ and $\mathbb{R}[x]$ since that polynomial has degree 2 but has no roots in $\mathbb{Q}$ or $\mathbb{R}$.

C) (5) In what sense are your factorizations from part B *unique*?

Solution: They are unique in the sense that any other irreducible factorization would consist of the same number of factors and each polynomial would be a nonzero constant times one of the polynomials in the given factorization. (The factors would match up after rearrangement, and up to multiplication by units.)

IV. Let $p(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$.

A) (15) Determine the addition and multiplication tables for the quotient ring $R = \mathbb{Z}_2[x]/(p(x))$.

Solution: The addition table is (writing, for instance, 1 for the coset $1 + (p(x))$):

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

The multiplication table is

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

B) (5) Is R a field? Why or why not?

Solution: The answer is *yes*. This can be seen directly by examining the multiplication table. Note that every nonzero element has a multiplicative inverse. It also follows from the result of Theorem 5.10 since the polynomial $p(x) = x^2 + x + 1$ is irreducible in $\mathbb{Z}_2[x]$.

C) (5) Show that $x + 1 \in \mathbb{Z}_2[x]/(p(x))$ is a root of the polynomial $y^2 + y + 1 \in \mathbb{Z}_2[y]$.

Solution: We compute directly with the addition and multiplication tables: If $y = x + 1$, then $y^2 = x$, so $y^2 + y + 1 = x + (x + 1) + 1 = 0$ since the coefficient arithmetic is done in $\mathbb{Z}_2$.

V.

A) (10) State the First Isomorphism Theorem for rings.

Solution: The First Isomorphism Theorem states that if $\varphi : R \to S$ is a ring homomorphism, then $\mathrm{im}(\varphi)$ is isomorphic to $R/\ker(\varphi)$ as a ring.

B) (10) Let φ be the mapping

$$\begin{aligned} \varphi : \mathbb{Z}[x] &\to \mathbb{Z}_3 \\ f(x) &\mapsto f(0) \bmod 3. \end{aligned}$$

(That is, φ takes each polynomial $f(x) = a_n x^n + \cdots + a_1 x + a_0$ to the class of a_0 mod 3). Show that φ is a ring homomorphism and show that its kernel is the ideal $(x, 3) \subset \mathbb{Z}[x]$.

Solution: φ is a ring homomorphism since

$$\begin{aligned} \varphi(f(x) + g(x)) &= [f(0) + g(0)](\text{class in } \mathbb{Z}_3) \\ &= [f(0)] + [g(0)], \end{aligned}$$

and

$$\begin{aligned} \varphi(f(x) \cdot g(x)) &= [f(0) \cdot g(0)] \\ &= [f(0)] + [g(0)] \bmod 3. \end{aligned}$$

The kernel of φ is the set of all $f(x)$ such that $\varphi(f(x)) = 0$ in $\mathbb{Z}_3$. Any polynomial in $(x, 3)$ is contained in the kernel since if $f(x) = xg(x) + 3h(x)$ for some $g(x), h(x)$, then $[f(0)] = [0 \cdot g(0) + 3h(0)] = [3h(0)] = [0]$. Conversely, if $[f(0)] = 0$, then $f(x) \in \mathbb{Z}[x]$ is a polynomial whose constant term is a multiple of 3. This means that we can write $f(x) = xg(x) + 3h(x)$ for polynomials $g(x), h(x)$. For instance, if $f(x) = a_n x^n + \cdots + a_1 x + a_0$, then $[f(0)] = [a_0] = 0$ so $a_0 = 3m$ for some $m \in \mathbb{Z}$. Hence $f(x) = x(a_n x^{n-1} + \cdots + a_1) + 3m \in (x, 3)$.

C) (5) Is the ideal $(x, 3)$ in $\mathbb{Z}[x]$ maximal? Why or why not?

Solution: The answer is *yes*. The homomorphism from part B is onto. Hence

$$\mathbb{Z}_3 \simeq \mathbb{Z}[x]/\ker(\varphi) = \mathbb{Z}[x]/(x, 3).$$

Since 3 is a prime number $\mathbb{Z}_3$ is a field, hence $(x, 3)$ is maximal.

VI. Let R be a ring with identity.

A) (7.5) Show that the set of units in R is a group under the multiplication operation from R.

Solution: We let U be the set of units in R, that is

$$U = \{r \in R : rs = 1 = sr \text{ for some } s \in R\}.$$

We must show that the gorup axioms hold in U. First U is closed under products since $(rs)^{-1} = s^{-1}r^{-1} \in U$ if $r \in U$ and $s \in U$. Associativity of multiplication follows from the ring axioms. U has an identity element since the ring multiplicative identity 1 serves that purpose. Finally, every element of U has a multiplicative inverse by definition. Hence U is a group under multiplication.

B) (10) Determine the multiplication table for the group of units in the ring $\mathbb{Z}_8 \times \mathbb{Z}_4 = \{(r, s) : r \in \mathbb{Z}_8 \text{ and } s \in \mathbb{Z}_4\}$ (componentwise sum and product).

Solution: The units in $\mathbb{Z}_8$ are $\{1, 3, 5, 7\}$ and the units in $\mathbb{Z}_4$ are $\{1, 3\}$. In order for $(a, b) \in \mathbb{Z}_8 \times \mathbb{Z}_4$ to be a unit, there must be some (c, d) such that $(a, b)(c, d) = (ac, bd) = (1, 1)$. Hence a and b must both be units themselves in their respective rings. The operation table is

$\cdot$	$(1,1)$	$(3,1)$	$(5,1)$	$(7,1)$	$(1,3)$	$(3,3)$	$(5,3)$	$(7,3)$
$(1,1)$	$(1,1)$	$(3,1)$	$(5,1)$	$(7,1)$	$(1,3)$	$(3,3)$	$(5,3)$	$(7,3)$
$(3,1)$	$(3,1)$	$(1,1)$	$(7,1)$	$(5,1)$	$(3,3)$	$(1,3)$	$(7,3)$	$(5,3)$
$(5,1)$	$(5,1)$	$(7,1)$	$(1,1)$	$(3,1)$	$(5,3)$	$(7,3)$	$(1,3)$	$(3,3)$
$(7,1)$	$(7,1)$	$(5,1)$	$(3,1)$	$(1,1)$	$(7,3)$	$(5,3)$	$(3,3)$	$(2,3)$
$(1,3)$	$(1,3)$	$(3,3)$	$(5,3)$	$(7,3)$	$(1,1)$	$(3,1)$	$(5,1)$	$(7,1)$
$(3,3)$	$(3,3)$	$(1,3)$	$(7,3)$	$(5,3)$	$(3,1)$	$(1,1)$	$(7,1)$	$(5,1)$
$(5,3)$	$(5,3)$	$(7,3)$	$(1,3)$	$(3,3)$	$(5,1)$	$(7,1)$	$(1,1)$	$(3,1)$
$(7,3)$	$(7,3)$	$(5,3)$	$(3,3)$	$(1,3)$	$(7,1)$	$(5,1)$	$(3,1)$	$(1,1)$

C) (7.5) Is your group from part B *cyclic*? Why or why not?

Solution: By inspection, we see that every element of this group has order 2. Hence it cannot be cyclic(!)

VII. *Note: This problem had a small but unfortunate error in its statement. It should have said:*

Let G be a group, and let H be a subgroup of G. Define

$$N_H = \{x \in G : xHx^{-1} = H\},$$

called the *normalizer of* H in G.

The condition $xHx^{-1} \subseteq H$ is enough to imply $xHx^{-1} = H$ when H is a finite group and in some other cases, but not in complete generality. The condition $xHx^{-1} = H$ is needed for one part below.

A) (10) Let $G = \mathrm{GL}(2, \mathbb{R})$ be the group of 2×2 invertible matrices under matrix multiplication and let

$$H = \left\{ \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} : r \in \mathbb{R} \right\}.$$

Show that H is a subgroup of G and determine N_H in this case.

Solution: First we show H is a subgroup. H is clearly nonempty since H contains one matrix for each real r. H is closed under matrix products since

$$\begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & r' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & r+r \\ 0 & 1 \end{pmatrix} \in H.$$

Also, H is closed under inverses since

$$\begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -r \\ 0 & 1 \end{pmatrix} \in H.$$

This shows that H is a subgroup of $\mathrm{GL}(2,\mathbb{R})$.

Next, we show that N_H is the set of upper-triangular invertible matrices,

$$B = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, b, d \in \mathbb{R}, ad \neq 0 \right\}.$$

First, we see that

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}^{-1} = \begin{pmatrix} \frac{1}{a} & \frac{-b}{ad} \\ 0 & \frac{1}{d} \end{pmatrix}.$$

So

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{a} & \frac{-b}{ad} \\ 0 & \frac{1}{d} \end{pmatrix} = \begin{pmatrix} 1 & \frac{ar}{d} \\ 0 & 1 \end{pmatrix}$$

which is in H. Moreover every matrix in H can be obtained. Hence $B \subseteq N_H$. Conversely, if $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is in N_H, then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} \cdot \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} * & * \\ \frac{-c^2 r}{ad-bc} & * \end{pmatrix}$$

is in H for all r. Looking at the lower left entry, we see that c must be 0. Hence the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is in B, so $N_H \subseteq B$.

B) (10) Show that for any subgroup of a general group, $H \subseteq G$, N_H is a subgroup of G containing H, and that H is a normal subgroup of N_H.

Solution: First, N_H contains H (and hence is nonempty). Indeed, if $y \in H$, since H is a subgroup (closed under products and inverses), $yxy^{-1} \in H$ for all $x \in H$. Hence $H \subseteq N_H$. Next, suppose that y, y' are both in N_H. Then $H = yHy^{-1} = H$, so $H = y'(yHy^{-1})(y')^{-1} = (y'y)H(y'y)^{-1}$. Hence $y'y \in N_H$. Finally, if $y \in N_H$, then $yHy^{-1} = H$. It follows that $y^{-1}Hy = H$ as well. This shows that $y^{-1} \in N_H$, so N_H is subgroup of G.

H is a normal subgroup of N_H since for all $y \in N_H$, $yHy^{-1} = H$. Hence one of the equivalent conditions of Theorem 7.34 holds.

C) (5) Show that the quotient group N_H/H for G, H as in part A is isomorphic to the group $\mathbb{R}^* \times \mathbb{R}^*$, where $\mathbb{R}^*$ denotes the multiplicative group of nonzero real numbers.

Solution: Define

$$\begin{array}{rcl} \varphi : N_H & \to & \mathbb{R}^* \times \mathbb{R}^* \\ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} & \mapsto & (a, d). \end{array}$$

The mapping φ is clearly onto. It is also a group homomorphism since

$$\begin{aligned} \varphi\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix}\right) &= \varphi\begin{pmatrix} aa' & ab' + bd' \\ 0 & dd' \end{pmatrix} \\ &= (aa', dd') \\ &= (a, d)(a', d') \\ &= \varphi\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\right)\varphi\left(\begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix}\right) \end{aligned}$$

The kernel of φ is the subset of N_H consisting of matrices with $a = d = 1$, which is just H. Then the statement we want follows from the First Isomorphism Theorem for groups.

VIII.

A) (5) By Lagrange's theorem, what are the possible orders of subgroups of S_4?

Solution: These are the divisors of $|S_4| = 24$:

$$|H| \in \{1, 2, 3, 4, 6, 8, 12, 24\}.$$

B) (10) Show that the subset $G \subset S_4$ defined by

$$G = \{(), (1234), (13)(24), (1432), (24), (1234)(24), (13)(24)(24), (1432)(24)\}$$

is a subgroup of S_4. Note that the second four elements are equal to the compositions of the first four with the two-cycle (24).

Solution: To do this in a reasonable way (i.e. without having to write out the whole 8×8 group table which is routine but tedious), note first that the first four elements are the elements of the cyclic subgroup $H = \langle(1234)\rangle \subset S_4$. The second four elements are these composed with (24). To show that G is closed under products, consider the four cases

- $\sigma\tau$,
- $\sigma(\tau(24))$,
- $(\sigma(24))\tau$, and
- $(\sigma(24))(\tau(24))$

for $\sigma, \tau \in H$. In the first case we have an element of $H \subset G$ since H is closed under products. In the second case, by associativity, $\sigma(\tau(24)) = (\sigma\tau)(24)$ and $\sigma\tau \in H$ so we have an element of G again. In the third case, note that $(\sigma(24))\tau = \sigma((24)\tau(24))(24)$ since (24) is an element of order 2 (equals its own inverse). The element $(24)\tau(24)$ the permutation obtained by interchanging 2,4 in τ. If $\tau = ()$ this changes nothing. If $\tau = (1234)$ then $(24)(1234)(24) = (1423) \in H$. If $\tau = (13)(24)$, then $(24)(13)(24)(24) = (13)(24) \in H$ again. If $\tau = (1432)$, then $(24)(1432)(24) = (1234)$. Hence all these elements give elements of G too (elements of the form $\sigma(24)$ for $\sigma \in H$). Finally in the fourth case, the reasoning used in case three shows that we obtain an element in H from $(24)\tau(24)$ so $\sigma(24)\tau(24) \in H \subset G$. Hence G is closed under products.

To show that G is closed under inverses, note that H is a subgroup of S_4 so the inverse of each element in H is also in H. The inverse of $\sigma(24)$ is $(24)\sigma^{-1} = (24)\sigma^{-1}(24)(24) = ((24)\sigma^{-1}(24))(24)$. This equals an element of H times (24) as in cases three and four of the proof for products.

- C) (10) Determine the left and right cosets of G in S_4. Is G a normal subgroup of S_4? Why or why not?

  Solution: The left cosets are (with elements written as products of disjoint cycles for easy comparison)

$$\begin{aligned} ()G = G &= \{(), (1234), (13)(24), (1432), (24), (12)(34), (13), (14)(23)\} \\ (12)G &= \{(12), (234), (1324), (143), (124), (34), (132), (1423)\} \\ (14)G &= \{(14), (123), (1342), (243), (142), (1243), (134), (23)\} \end{aligned}$$

  The right cosets are *different*

$$\begin{aligned} G() = G &= \{(), (1234), (13)(24), (1432), (24), (12)(34), (13), (14)(23)\} \\ G(12) &= \{(12), (134), (1423), (243), (142), (34), (123), (1324)\} \\ G(14) &= \{(14), (234), (1243), (132), (124), (1342), (143), (23)\} \end{aligned}$$

  This shows G is *not a normal subgroup of* S_4.

  Comment: G is isomorphic to D_4, the symmetries of the square, here!

Have a peaceful and joyous holiday season!