**Math 351**

**Solutions to review problems for Exam #2** **November 17, 2007**

Exam #2 will be given during the normal class period on Monday, November 19. It will cover material from Sections 4.5, 4.6, 5.1 - 5.3, 6.3, 9.1, 9.4, 7.1 - 7.4. This set of review problems is about twice as long as the exam. As usual, $\mathbf{Z}$ denotes the ring of integers, $\mathbf{Q}$ denotes the field of rational numbers, and $\mathbf{C}$ denotes the field of complex numbers.

#1 Let $f(x) \in \mathbf{R}[x]$ have degree 7. Prove that $f(x)$ is a reducible polynomial in $\mathbf{R}[x]$. You may want to use the fact that every irreducible polynomial in $\mathbf{C}[x]$ has degree 1.

**Solution:** Since $f(x) \in \mathbf{R}[x] \subset \mathbf{C}[x]$, we have

$$f(x) = a(x - b_1)(x - b_2)...(x - b_7)$$

for some $a, b_1, b_2, .., b_7 \in \mathbf{C}$. Since the coefficients of $f(x)$ are real, we also have

$$f(x) = \bar{a}(x - \bar{b}_1)(x - \bar{b}_2)...(x - \bar{b}_7),$$

where $\bar{u}$ denotes the complex conjugate of $u$. Thus $\bar{b}_1$ is a root of $f(x)$ and so is one of $b_1, ..., b_7$. If $\bar{b}_1 = b_1$ then $b_1 \in \mathbf{R}$, so $x - b_1 \in \mathbf{R}[x]$ and hence $f(x)$ is reducible in $\mathbf{R}[x]$. If $\bar{b}_1 = b_j$ for some $j, 2 \leq j \leq 7$ then $(x - b_1)(x - b_j) = (x - b_1)(x - \bar{b}_1) \in \mathbf{R}[x]$ and $f(x)$ is reducible in $\mathbf{R}[x]$.

#2 Let $f(x)$ and $g(x)$ be polynomials in $\mathbf{Z}[x]$. Let $p$ be a prime integer. Prove that if $p$ divides every coefficient of $f(x)g(x)$ then either $p$ divides every coefficient of $f(x)$ or $p$ divides every comefficient of $g(x)$.

**Solution:** Let $f(x) = a_n x^n + ... + a_1 x + a_0$ and $g(x) = b_m x^m + ... + b_1 x + b_0$. Assume $p$ does not divide every coefficient of $f(x)$ and does not divide every coefficient of $g(x)$. Then we may find $i, 0 \leq i \leq n$, such that $p|a_k$ for $0 \leq k < i$, but $p \not| a_i$. We may also find $j, 0 \leq j \leq m$, such that $p|b_k$ for $0 \leq k < j$, but $p \not| b_j$. Write $a_l = 0$ if $l > n$ and $b_l = 0$ if $l > m$. Then the coefficient of $x^{i+j}$ in $f(x)g(x)$ is $\sum_{l=0}^{i+j} a_l b_{i+j-l}$. Since $p|a_l$ whenever $l < i$ and $p|b_{i+j-l}$ whenever $l > i$ we see that the coefficient of $x^{i+j}$ in $f(x)g(x)$ is congruent to $a_i b_j$ modulo $p$. But $p \not| a_i b_j$.

#3 Let $f(x) = a_n x^n + ... + a_1 x + a_0 \in \mathbf{Z}[x]$ and suppose that $\frac{r}{s} \neq 0$ is a root of $f(x)$ where $r, s \in \mathbf{Z}$ and $r$ and $s$ are relatively prime. Prove that $r|a_0$ and $s|a_n$.

**Solution:** We have $0 = s^n f(\frac{r}{s}) = a_n r^n + a_{n-1} r^{n-1} s + a_{n-2} r^{n-2} s^2 + ... + a_1 r s^{n-1} + a_0 s^n$. Thus

$$a_n r^n = -(a_{n-1} r^{n-1} s + a_{n-2} r^{n-2} s^2 + ... + a_1 r s^{n-1} + a_0 s^n) =$$

$$-s(a_{n-1} r^{n-1} + a_{n-2} r^{n-2} s + ... + a_1 r s^{n-2} + a_0 s^{n-1}).$$

Thus $s|a_n r^n$ and, since $(r, s) = 1$, $r|a_n$. Similarly

$$a_0 s^n = -(a_n r^n + ... + a_1 r s^{n-1}) = -r(a_n r^{n-1} + ... + a_1 s^{n-1})$$

and so $r|a_0$.

#4 Let $f(x) \in \mathbf{Z}[x]$ and assume that $f(x)$ is an irreducible polynomial in $\mathbf{Z}[x]$. Prove that $f(x)$ is an irreducible polynomial in $\mathbf{Q}[x]$. You may want to use the results of problems #2 and #3.

**Solution:** We will assume that $f(x) \in \mathbf{Z}[x]$ is reducible in $\mathbf{Q}[x]$, say $f(x) = g(x)h(x)$ where $g(x), h(x) \in \mathbf{Q}[x]$ are polynomials of degree $\geq 1$, and show that $f(x)$ is reducible in $\mathbf{Z}[x]$. First note that there are integers $m$ and $n$ such that $mg(x), nh(x) \in \mathbf{Z}[x]$. Thus $mnf(x) = (mg(x))(nh(x))$ is reducible in $\mathbf{Z}[x]$. Let $S$ denote the set of all positive integers $l$ such that $lf(x)$ is reducible in $\mathbf{Z}[x]$. Then $mn \in S$, so $S$ is nonempty. Hence $S$ contains a smallest element $k$. If $k > 1$ then some prime $p$ divides $k$ and hence $p$ divides every coefficient of $kf(x)$. Since $kf(x)$ is reducible in $\mathbf{Z}[x]$ we have $kf(x) = r(x)s(x)$ for some polynomials $r(x), s(x) \in \mathbf{Z}[x]$ of degree $\geq 1$. Then, by the result of problem #2, either $p$ divides every coefficient of $r(x)$ or $p$ divides every coefficient of $s(x)$. In the first case $\frac{1}{p}r(x) \in \mathbf{Z}[x]$ and so $\frac{k}{p}f(x) = (\frac{1}{p}r(x))(s(x))$ is reducible in $\mathbf{Z}[x]$. This contradicts the minimality of $k$. In the second case $\frac{1}{p}s(x) \in \mathbf{Z}[x]$ and so $\frac{k}{p}f(x) = (r(x))(\frac{1}{p}s(x))$ is reducible in $\mathbf{Z}[x]$. Again, this contradicts the minimality of $k$. Thus $k = 1$ and the proof is complete.

#5 Show (by constructing an example) that there is a field with 8 elements.

**Solution:**

Suppose $f(x)$ is an irreducible polynomial of degree 3 over the field $\mathbf{Z}_2$. Then $F = \mathbf{Z}[x]/(f(x))$ is a field whose elements are all the cosets of the ideal $f(x)$. Now if $g(x) \in \mathbf{Z}_2[x]$ we may write $g(x) = q(x)f(x) + r(x)$ where $q(x), r(x) \in \mathbf{Z}_2[x]$ and either $r(x) = 0$ or $r(x)$ has degree $\leq 2$. Then the coset $g(x) + (f(x))$ is equal to the coset $r(x) + (f(x))$ and so the number of elements in $F$ is equal to the number of possible $r(x)$. Since there are only 2 choices (in $\mathbf{Z}_2$) for each of the 3 coefficients of $r(x)$, we see that $F$ has 8 elements. Thus we only need to find an irreducible polynomial of degree 3 over $\mathbf{Z}_2$. Since a polynomial of degree 3 is reducible if and only if it has a root, we simply need to find a polynomial $f(x) = x^3 + ax^2 + bx + c$ such that $f(0) \neq 0, f(1) \neq 0$. Since $\mathbf{Z}_2$ has only two elements (0 and 1), this means that $c = f(0) = 1, 1 + a + b + c = f(1) = 1$. Thus $f(x)$ is irreducible if and only if $c = 1$ and $a + b = 1$. Thus there are two irreducible polynomials of degree 3 over $\mathbf{Z}_2$: $x^3 + x^2 + 1$ and $x^3 + x + 1$.

#6 Let $F$ be a field and $f(x) \in F[x]$. Let $p(x) \in F[x]$ be a polynomial of degree $\geq 1$. Prove that $f(x) + (p(x))$ is a unit in $F[x]/(p(x))$ if and only if $f(x)$ and $p(x)$ are relatively prime.

**Solution:** $f(x) + (p(x))$ is a unit in $F[x]/(p(x))$ if and only if there is some $g(x) \in F[x]$ such that $f(x)g(x) + (p(x)) = (f(x) + (p(x)))(g(x) + (p(x)) = 1 + (p(x))$. This happens if and only if $f(x)g(x) - 1 \in (p(x))$ and this is equivalent to $f(x)g(x) - 1 = k(x)p(x)$ for some $k(x) \in F[x]$. This may be rewritten as $f(x)g(x) - p(x)k(x) = 1$. But this condition holds if and only if $f(x)$ and $p(x)$ are relatively prime.

#7 (a) State the definition a prime ideal in a ring $R$.

(b) Prove that an ideal $I$ in a commutative ring $R$ with identity is a prime ideal if and only if $R/I$ is an integral domain.

(c) State the definition of a maximal ideal in a ring $R$.

(d) Prove that if $R$ is a commutative ring with identity, then an ideal $I$ in $R$ is maximal if and only if $R/I$ is a field.

**Solution:**

(a) An ideal $I \subseteq R$ is prime if whenever $a, b \in R, ab \in I$ we have either $a \in I$ or $b \in I$.

(b) Suppose $I$ is prime ideal in $R$. Let $a+I, b+I \in R/I$ and assume $(a+I)(b+I) = 0$ in $R/I$. Then $ab+I = I$ so $ab \in I$. Since $I$ is prime, either $a \in I$ or $b \in I$ and hence either $a+I = 0$ or $b+I = 0$ in $R/I$. Hence $R/I$ is an integral domain. Conversely, suppose $R/I$ is an intgral domain and $a, b \in R, ab \in I$. Then $(a+I)(b+I) = ab+I = I = 0$ in $R/I$ so either $a+I = 0$ or $b+I = 0$ in $R/I$. Thus either $a \in I$ or $b \in I$, so $I$ is a prime ideal.

(c) An ideal $I \subseteq R$ is a maximal ideal in $R$ if $I \neq R$ whenever $J$ is an ideal of $R$ with $I \subseteq J \subseteq R$ then either $J = I$ or $J = R$.

(d) Let $S$ be a commutative ring with identity. If $S$ is the only nonzero ideal of $S$ and if $0 \neq a \in S$ then $(a) = S$ so $1 \in (a)$. Thus $1 = ab$ for some $b \in S$ and so $S$ is a field. Conversely, if $S$ is a field any nonzero ideal must contain 1 and so must equal $S$. Since an ideal $I \subseteq R$ is maximal if and only if $R/I$ is the only nonzero ideal of $R/I$ we have the result.

#8 Show that $\mathbf{Z}[\sqrt{-2}]$ is a Euclidean domain with $\delta(a + b\sqrt{-2}) = a^2 + 2b^2$.

**Solution:** Write $R = \mathbf{Z}[\sqrt{-2}]$. $R$ is a subring of the field $\mathbf{Q}[\sqrt{-2}]$, so it is an integral domain. Thus to show $R$ is a Euclidean domain we must verify two conditions on $\delta$: (i) If $u, v \in R$ then $\delta(u) \leq \delta(uv)$; (ii) If $u, v \in R, v \neq 0$ then $u = qv + r$ for some $q, r \in R$ with $r = 0$ or $\delta(r) < \delta(v)$.Now for $u = a + b\sqrt{-2} \in R \subseteq \mathbf{C}$ we have $\bar{u}$, the complex conjugate of $u$, is $a - b\sqrt{-2}$ and $\delta(u) = u\bar{u}$. Thus for $u, v \in R$ we have $\delta(uv) = (uv)(\overline{uv}) = (u\bar{u})(v\bar{v}) = \delta(u)\delta(v)$ and so $\delta(u) \leq \delta(uv)$. Thus the first condition holds. To verify the second condition assume $v \neq 0$ and note that, since $\mathbf{Q}[\sqrt{-2}]$ is a field, $u = (w_1 + w_2\sqrt{-2})v$ for some $w_1, w_2 \in \mathbf{Q}$. Then we may find $q_1, q_2 \in \mathbf{Z}$ such that $|w_1 - q_1| \leq \frac{1}{2}, |w_2 - q_2| \leq \frac{1}{2}$. Set $q = q_1 + q_2\sqrt{-2}$ and set $r = u - qv$. We must show that either $r = 0$ or $\delta(r) < \delta(v)$. Now $r = u - qv = (w_1 + w_2\sqrt{-2})v - qv = ((w_1 - q_1) + (w_2 - q_2)\sqrt{-2})v$. Then writing $v = v_1 + v_2\sqrt{-2}$ we have

$$r = ((w_1 - q_1) + (w_2 - q_2)\sqrt{-2})(v_1 + v_2\sqrt{-2}) =$$

$$((w_1 - q_1)v_1 - 2(w_2 - q_2)v_2) + ((w_1 - q_1)v_2 + (w_2 - q_2)v_1)\sqrt{-2}$$

and so

$$\delta(r) = ((w_1 - q_1)v_1 - 2(w_2 - q_2)v_2)^2 + 2((w_1 - q_1)v_2 + (w_2 - q_2)v_1)^2 =$$

$$(w_1 - q_1)^2 v_1^2 - 4(w_1 - q_1)v_1(w_2 - q_2)v_2 + 4(w_2 - q_2)^2 v_2^2 +$$

$$2(w_1 - q_1)^2 v_2^2 + 4(w_1 - q_1)v_2(w_2 - q_2)v_1 + 2(w_2 - q_2)^2 v_1^2 =$$

$$((w_1 - q_1)^2 + 2(w_2 - q_2)^2)v_1^2 + (4(w_2 - q_2)^2 + 2(w_1 - q_1)^2)v_2^2 \leq$$
$$\frac{3}{4}v_1^2 + \frac{3}{2}v_2^2 < \delta(v).$$

#9 Let $R$ be an integral domain. Define $S = \{(a, b)|a, b \in R, b \neq 0\}$. Define $(a, b) \sim (c, d)$ if $ad = bc$. Show that $\sim$ is an equivalence relation.

**Solution:**

Reflexivity: Since $ab = ba$ we have $(a, b) \sim (a, b)$.

Symmetry: Assume $(a, b) \sim (c, d)$. Then $ad = bc$ and so $cb = da$. Hence $(c, d) \sim (a, b)$.

Transitivity: Assue $(a, b) \sim (c, d), (c, d) \sim (e, f)$. Then $ad = bc$ and $cf = de$. Multiplying the first equalty by $f$ gives $adf = bcf$ and multiplying the second by $b$ gives $bcf = bde$. Thus $adf = bde$. Hence $0 = adf - bde = d(af - be)$. Since $R$ is an integral domain and $d \neq 0$ we have $af - be = 0$ so $af = be$ and hence $(a, b) \sim (e, f)$.

#10 Let $R = \{a + b\sqrt{3}|a, b \in \mathbf{Z}\}$. Then $R$ is an integal domain (why?) and so $R$ has a quotient field $F$. What is $F$?

**Solution:** $R$ is a subring of the field of real numbers and is therefore an integral domain. Let $E = \{a + b\sqrt{3}|a, b \in \mathbf{Q}\}$. Note that if $0 \neq a + b\sqrt{3} \in E$ then

$$(a + b\sqrt{3})(a - b\sqrt{3}) = a^2 - 3b^2$$

is a rational number and is nonzero (since $\sqrt{3}$ is irrational). Thus

$$(a + b\sqrt{3})^{-1} = \frac{(a - b\sqrt{3})}{a^2 - 3b^2}.$$

Hence $E$ is a subfield of the field of real numbers. Then by Theorem 9.31, $E$ contains a subfield isomorphic to $F$. But any subfield of the real numbers containing $R$ must contain all rational numbers and must contain $\sqrt{3}$, so it must contain $E$. Thus $F$ is isomorphic to $E$.

#11 Let $G$ be a group, $g, h, k \in G$ and $gh = gk$. Prove that $h = k$. Conclude that the multiplicative inverse of $g$ is unique.

**Solution:** Since $G$ is a group, it contains an identity element $e$ and some element $u$ such that $ug = e$. Then $h = eh = (ug)h = u(gh) = u(gk) = (ug)k = ek = k$. Now suppose $u, v \in G$ are inverses of $g$. Then $gu = e = gv$ and so we have $u = v$.

#12 Compute the product

$$(\begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 6 & 1 & 2 & 3 & 7 & 5 \end{matrix})(\begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 1 & 5 & 6 & 7 \end{matrix})$$

in the symmetric group on 7 elements.

**Solution:**

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 1 & 2 & 4 & 3 & 7 & 5 \end{pmatrix}$

#13 Let $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 7 & 6 & 4 & 1 & 3 \end{pmatrix}$ in the symmetric group on 7 elements.

(a) Find $g^{-1}$.

(b) Find the order of $g$.

**Solution:**

(a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 1 & 7 & 5 & 2 & 4 & 3 \end{pmatrix}$

(b) Note that $g(1) = 2, g^2(1) = g(2) = 5, g^3(1) = g(5) = 4, g^4(1) = g(4) = 6, g^5(1) = g(6) = 1$. Thus $g^k(1) = 1$ if and only if $5|k$. This computation also shows that $g^5(2) = 2, g^5(5) = 5, g^5(4) = 4$, and $g^5(6) = 6$. Similarly $g(3) = 7, g^2(7) = 3$ and so $g^k(3) = 3$ if and only if $2|k$ and the computation also shows that $g^2(7) = 7$. Thus 10 must divide the order of $g$ and $g^{10}$ is the identity permuation. Thus the order of $g$ is 10.

#14 Let $G$ be a group with identity element $e$. Suppose $g^2 = e$ for all $g \in G$. Prove that $G$ is commutative.

**Solution:** Here are two slightly different proofs:

(i) Multiply both sides of $g^2 = e$ by $g^{-1}$ to get $g = g^{-1}$ for all $g \in G$. Now let $g, h \in G$ and recall that $(gh)^{-1} = h^{-1}g^{-1}$. Then

$$gh = (gh)^{-1} = h^{-1}g^{-1} = hg.$$

(ii) Let $g, h \in G$. Then $(gh)^2 = ghgh = e$. Also $g^2 = h^2 = e$ so $g^2h^2 = e$. Hence $ghgh = gghh$. Multiply on the left by $g^{-1}$ to get $hgh = ghh$ and then multiply on the right by $h^{-1}$ to get $hg = gh$.

#15 Let $G$ be a commutative group with identity element $e$ and let $n \in \mathbf{Z}, n \geq 1$. Let $H = \{g \in G | g^n = e\}$. Prove that $H$ is a subgroup of $G$.

**Solution:** Since $e \in H$, we have that $H$ is nonempty. If $g, h \in H$, then $(gh)^n = g^n h^n = ee = e$, so $gh \in H$. Also, $(g^{-1})^n = g^{-n} = (g^n)^{-1} = e^{-1} = e$, so $g^{-1} \in H$. Thus $H$ is a subgroup.