**Math 351**

**Solutions to review problems for Final Exam** **December 16, 2007**

#1 Find $(78, 2340)$ and write it in the form $78a + 2340b$ where $a$ and $b$ are integers.

**Solution:**

$$2370 = 30(78) + 30 \textit{ and so } 30 = 2370 - 30(78)$$

$$78 = 2(30) + 18 \textit{ and so } 18 = 78 - 2(30)$$

$$30 = 18 + 12 \textit{ and so } 12 = 30 - 18$$

$$18 = 12 + 6 \textit{ and so } 6 = 18 - 12$$

$$12 = 2(6) + 0.$$

Thus $(78, 2370) = 6$. Furthemore

$$6 = 18 - 12 = (18 - (30 - 18) = -30 + 2(18) =$$

$$-30 + 2(78 - 2(30)) = 2(78) - 5(30) =$$

$$2(78) - 5(2370 - 30(78)) = -5(2370 + 152(78).$$

#2 Find $[12]^{-1}$ in $\mathbf{Z}_{25}$.

**Solution:** $25 = 2(12) + 1$ so

$$1 - (-2)(12) = 25$$

and hence

$$1 \equiv (-2)(12) \ mod(25).$$

Thus

$$[1] = [-2][12] \ in \mathbf{Z}_{25}.$$

Hence

$$[12]^{-1} = [-2] = [23] \ in \mathbf{Z}_{12}.$$

#3 Let $R$ be a ring and $A, B$ be ideals in $R$. Let $A + B$ denote $\{a + b | a \in A, b \in B\}$

(a) Prove that $A + B$ is an ideal in $R$.

(b) Recall that if $n \in \mathbf{A}$, then $(n)$ denotes $\{nk | k \in \mathbf{Z}\} = n\mathbf{Z}$. Prove that any ideal in $\mathbf{Z}$ is equal to $(n)$ for some $n \in \mathbf{Z}, n \geq 0$.

(c) Let $m, n \in \mathbf{Z}, m, n > 0$. Prove that $(m) + (n) = ((m, n))$. (Recall that $(m, n)$ denotes the greatest common divisor of $m$ and $n$.)

**Solution:**

(a) Let $c_1, c_2 \in A + B$ and $r \in R$. Then $c_1 = a_1 + b_1$ and $c_2 = a_2 + b_2$ for some $a_1, a_2 \in A, b_1, b_2 \in B$. Then $c_1 - c_2 = (a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2)$. Since $A$ and $B$ are ideals (and hence subrings) $a_1 - a_2 \in A$ and $b_1 - b_2 \in B$. Thus $c_1 - c_2 \in A + B$.

Also $rc_1 = r(a_1 + b_1) = ra_1 + rb_1$. Since $A$ and $B$ are ideals, $ra_1 \in A$ and $rb_1 \in B$. Thus $rc_1 \in A + B$. Similarly $c_1 r = a_1 r + b_1 r \in A + B$. Thus $A + B$ is an ideal

(b) Let $I$ be an ideal in $\mathbf{Z}$. If $I = \{0\}$ then $I = (0)$ and we are done. If not, $I$ contains a nonzero integer and (since $a \in I$ implies $(-1)a \in I$) $I$ contains a positive integer. Thus the set of positive integers in $I$ is nonempty and so this set contains a smallest integer. Let this smallest integer in $I$ be $n$. Since $n \in I$ we have $(n) \subseteq I$. Now let $k \in I$. Then $k = qn + r$ for some $q, r \in \mathbf{Z}$ with $0 \leq r < n$. But $r = k - qn \in I$, so, since $n$ is the smallest positive integer in $I$, we must have $r = 0$. Thus $k = qn \in (n)$ so we have $I \subseteq (n)$ and hence $I = (n)$.

(c) By part (a), $(m) + (n)$ is an ideal and by part (b) we have $(m) + (n) = (k)$ for some positive integer $k$. We must show that $k = (m, n)$. We know that $(m, n) = am + bn$ for some $a, b \in \mathbf{Z}$ and so $(m, n) \in (m) + (n) = (k)$. Thus $k|(m, n)$. But $k \in (k) = (m) + (n)$ and $(m, n)$ divides both $m$ and $n$, so $(m, n)|k$. Thus $(m, n) = k$ as required.

#4 Find all the ideals in $\mathbf{Z}_{10} \times \mathbf{Z}$. Which of these are prime ideals? Which of these are maximal ideals?

**Solution:** Let $R = \mathbf{Z}_{10} \times \mathbf{Z}$. Note that $R_1 = \mathbf{Z}_{10} \times (0) \subseteq \mathbf{Z}_{10} \times \mathbf{Z}$ and $R_2 = (0) \times \mathbf{Z} \subseteq \mathbf{Z}_{10} \times \mathbf{Z}$ are ideals in $R$. Then if $I$ is any ideal in $R$ we have that $I_1 = R_1 \cap I$ and $I_2 = R_2 \cap I$ are ideals in $R$. But if $(a, b) \in I$ then $(a, b) = (a, 0) + (0, b) = (a, b)(1, 0) + (a, b)(0, 1) \in I_1 + I_2$. Since $I_1$ is isomorphic to an ideal in $\mathbf{Z}_{10}$ (hence to $([k])$ where $k = 0, 1, 2, 5$) and $I_2$ is isomorphic to an ideal in $\mathbf{Z}$ (hence to $(n)$ where $n \in \mathbf{Z}, n \geq 0$). Now $(1, 0)(0, 1) = (0, 0)$ in $R$ and so the quotient of $R$ by $([k]) \times (n)$ will have zero divisors unless $k = 1$ or $n = 1$. Now $\mathbf{Z}/([k])$ is an integral domain if and only if $k = 2$ or $5$ and in this case it is a field. Furthermore, $\mathbf{Z}/(n)$ is an integral domain if and if either $n$ is prime (in which case it is a field) or if $n = 0$ (in which case it is not a field). Thus the prime ideals are $([k]) \times \mathbf{Z}$ for $k = 2, 5$, $\mathbf{Z}_{10} \times (p)$ for $p$ prime, and $\mathbf{Z}_{10} \times (0)$. All of these except the last are also maximal.

#5 Find $[x^2 + x + 1]^{-1}$ in $\mathbf{Q}[x]/(x^3 + 2)$.

**Solution:** $x^3 + 2 = (x - 1)(x^2 + x + 1) + 3$. Thus

$$1 = (\frac{-1(x-1)}{3})(x^2 + x + 1) + \frac{x^3 + 2}{3}$$

and so

$$[1] = [\frac{-1(x-1)}{3}][x^2 + x + 1].$$

Thus $[x^2 + x + 1]^{-1} = [\frac{-1(x-1)}{3}]$.

#6 Find $(x^3 + 2x^2 - x - 2, x^4 - 1)$ in $\mathbf{Q}[x]$ and exrpess it in the form $(x^3 + 2x^2 - x - 2)a + (x^4 - 1)b$ where $a, b \in \mathbf{Q}[x]$.

**Solution:**

$$x^4 - 1 = (x - 2)(x^3 + 2x^2 - x - 2) + 5(x^2 - 1)$$

and so

$$x^2 - 1 = (\frac{-(x-2)}{5})(x^3 + 2x^2 - x - 2) + \frac{(x^4 - 1)}{5},$$

and

$$x^3 + 2x^2 - x - 2 = (x+2)(x^2 - 1).$$

Thus $x^2 - 1 = (x^3 + 2x^2 - x - 2, x^4 - 1)$.

#7 (a) Let $R = \{A \in M_2(\mathbf{R}) | A \begin{vmatrix} 1 \\ -1 \end{vmatrix} = \begin{vmatrix} 0 \\ 0 \end{vmatrix}\}$. Show that $A$ is a subring of $M_2(\mathbf{R})$ but that $A$ is not an ideal.

(b) Let $S = \{B \in M_2(\mathbf{R}) | B \begin{vmatrix} 1 \\ -1 \end{vmatrix} \in \mathbf{R} \begin{vmatrix} 1 \\ -1 \end{vmatrix}\}$. Show that $S$ is a subring of $M_2(\mathbf{R})$.

(c) Show that $R$ is an ideal in $S$ and that $S/R$ is isomorphic to $\mathbf{R}$.

**Solution:**

(a) Let $A_1, A_2 \in R$. Then

$$(A_1 - A_2) \begin{vmatrix} 1 \\ -1 \end{vmatrix} = A_1 \begin{vmatrix} 1 \\ -1 \end{vmatrix} - A_2 \begin{vmatrix} 1 \\ -1 \end{vmatrix} = \begin{vmatrix} 0 \\ 0 \end{vmatrix}$$

and

$$(A_1 A_2) \begin{vmatrix} 1 \\ -1 \end{vmatrix} = A_1 (A_2 \begin{vmatrix} 1 \\ -1 \end{vmatrix}) = A_1 \begin{vmatrix} 0 \\ 0 \end{vmatrix} = \begin{vmatrix} 0 \\ 0 \end{vmatrix}.$$

Hence $A_1 - A_2 \in R$ and $A_1 A_2 \in R$, so $R$ is a subring. However $\begin{vmatrix} 1 & 1 \\ 1 & 1 \end{vmatrix} \in R$ but

$$\begin{vmatrix} 1 & 1 \\ 1 & 1 \end{vmatrix} \begin{vmatrix} 1 & 0 \\ 0 & -1 \end{vmatrix} = \begin{vmatrix} 1 & -1 \\ 1 & -1 \end{vmatrix} \notin R.$$

Thus $R$ is not an ideal.

(b) Let $B_1, B_2 \in S$. Thus $B_1 \begin{vmatrix} 1 \\ -1 \end{vmatrix} = k_1 \begin{vmatrix} 1 \\ -1 \end{vmatrix}$ and $B_2 \begin{vmatrix} 1 \\ -1 \end{vmatrix} = k_2 \begin{vmatrix} 1 \\ -1 \end{vmatrix}$ for some $k_1, k_2 \in \mathbf{R}$. Then

$$(B_1 - B_2) \begin{vmatrix} 1 \\ -1 \end{vmatrix} = B_1 \begin{vmatrix} 1 \\ -1 \end{vmatrix} - B_2 \begin{vmatrix} 1 \\ -1 \end{vmatrix} = k_1 \begin{vmatrix} 1 \\ -1 \end{vmatrix} - k_2 \begin{vmatrix} 1 \\ -1 \end{vmatrix} = (k_1 - k_2) \begin{vmatrix} 1 \\ -1 \end{vmatrix}$$

and

$$(B_1 B_2) \begin{vmatrix} 1 \\ -1 \end{vmatrix} = B_1 (B_2 \begin{vmatrix} 1 \\ -1 \end{vmatrix}) = B_1 (k_2 \begin{vmatrix} 1 \\ -1 \end{vmatrix} = k_2 B_1 \begin{vmatrix} 1 \\ -1 \end{vmatrix} = k_1 k_2 \begin{vmatrix} 1 \\ -1 \end{vmatrix}.$$

Thus $S$ is a subring.

(c) Let $A \in R$ and $B \in S$ with $B \begin{vmatrix} 1 \\ -1 \end{vmatrix} = k \begin{vmatrix} 1 \\ -1 \end{vmatrix}$. Then

$$(BA) \begin{vmatrix} 1 \\ -1 \end{vmatrix} = B(A \begin{vmatrix} 1 \\ -1 \end{vmatrix}) = B( \begin{vmatrix} 0 \\ 0 \end{vmatrix}) = \begin{vmatrix} 0 \\ 0 \end{vmatrix}$$

and

$$(AB) \begin{vmatrix} 1 \\ -1 \end{vmatrix} = A(B \begin{vmatrix} 1 \\ -1 \end{vmatrix}) = A(k \begin{vmatrix} 0 \\ 0 \end{vmatrix}) = kA \begin{vmatrix} 1 \\ -1 \end{vmatrix} = k \begin{vmatrix} 0 \\ 0 \end{vmatrix} = \begin{vmatrix} 0 \\ 0 \end{vmatrix}.$$

Thus $R$ is an ideal in $S$. Now define $\theta : S \to \mathbf{R}$ by $B \begin{vmatrix} 1 \\ -1 \end{vmatrix} = \theta(B) \begin{vmatrix} 1 \\ -1 \end{vmatrix}$. It is easy to check that $\theta$ is a surjective homomorphism with kernel $R$. Thus the First Isomorphism Theorem gives that $S/R$ is isomorphic to $\mathbf{R}$.

#8 Let $F$ be a field and $I_1 \subseteq I_2 \subseteq I_3 \subseteq ...$ be ideals of $F[x]$. Show that there is some $k$ such that $I_k = I_{k+1} = ....$

**Solution:** Any ideal in $F[x]$ is equal to $(f(x))$ where $f(x)$ is either 0 or some monic polynomial $f(x)$. Thus we may find $f_1(x), f_2(x), ...$ such that $I_j = (f_j(x))$ for all $j$. Then $f_j(x) \in (f_j(x)) = I_j \subseteq I_{j+1} = (f_{j+1}(x))$ and so $f_j(x) = q_j(x)f_{j+1}(x)$ for some polynomial $q_j(x)$. If $f_j(x) \neq 0$, this implies $deg(f_j(x)) \geq deg(f_{j+1}(x))$ and so $deg(f_j(x)) \geq deg(f_{j+l}(x)$ for all $l \geq 0$.Consider $S = \{deg(f_j(x)) | f_j(x) \neq 0, j \geq 1\}$. If $S = \emptyset$ then every $I_j = (0)$ and so the result holds. If $S$ is not empty it contains a minimal element, say $deg(f_k(x))$. We already know $deg(f_k(x)) \geq deg(f_{k+l}(x))$ for all $l \geq 0$, so the minimality of $deg(f_k(x))$ implies $deg(f_k(x)) = deg(f_{k+l}(x))$ for all $l \geq 0$. Since $f_k(x) \in (f_k(x)) = I_k \subseteq I_{k+l} = (f_{k+l}(x))$ we see that $f_{k+l}(x)$ divides $f_k(x)$. Since these are monic polynomials of the same degree, they are equal. Thus $f_k(x) = f_{k+1}(x) = ...$ and so $I_k = I_{k+1} = ...$

#9 (a) Is $x^5 + 3x^4 + 6x^2 - 9x + 3$ irreducible over $\mathbf{Q}$? Why or why not?
(b) Is $x^5 + x^4 + 1$ irreducible over $\mathbf{Z}_2$? Why or why not?

**Solution:**
(a) A polynomial in $\mathbf{Z}[x]$ is irreducible over $\mathbf{Q}$ if and only if it is irreducible over $\mathbf{Z}$. The given polynomial is irreducible over $\mathbf{Z}$ by Eisenstein's criterion (with $p = 3$).
(b) Note that the polynomial has no roots (since 0 and 1 are the only possibilities and neither is a root). Since the polynomial is of degree five, it can be reducible only if it is the product of an irreducible polynomial of degree 2 and an irreducible polynomial of degree 3. Now there is only one irreducible polynomial of degree 2 in $\mathbf{Z}_2[x]$, namely $x^2+x+1$ (because there are only 4 polynomials of degree 4 in $\mathbf{Z}_2[x]$ and the other 3 all have roots). Thus if $x^5 + x^4 + 1$ is reducible we must have $x^5 + x^4 + 1 = (x^3 + ax^2 + bx + c)(x^2 + x + 1)$ for some $a, b, c \in \mathbf{Z}_2$. Writing out the product and comparing coefficients gives $a = 0, b = c = 1$. Thus $x^5 + x^4 + 1 = (x^3 + x + 1)(x^2 + x + 1)$ in $\mathbf{Z}_2[x]$, so the polynomial is reducible.

#10 Let $R$ be a ring and $I$ be an ideal in $R$. Prove that every subring of $R/I$ has the form $J/I$ where $J$ is a subring of $R$ which contains $I$. Also show that $J$ is an ideal in $R$ if and only if $J/I$ is an ideal in $R/I$.

**Solution:** Let $A$ be a subring in $R/I$. Define $\bar{A} = \{r \in R | r + I \in A\}$. Let $a_1, a_2 \in \bar{A}$. Then $a_1 + I, a_2 + I \in A$ and so $(a_1 - a_2) + I = (a_1 + I) - (a_2 + I) \in A$ and $(a_1a_2) + I = (a_1 + I)(a_2 + I) \in A$. Thus $a_1 - a_2, a_1a_2 \in \bar{A}$ and so $\bar{A}$ is a subring of $R$. Now if $b \in I$ we have $b + I = 0 + I = 0_{R/I} \in A$. Thus $b \in \bar{A}$ and so $I \subseteq \bar{A}$. Then $I$ is an ideal in $\bar{A}$ and $\bar{A}/I = \{a + I | a \in \bar{A}\} = A$. Furthermore, if $A$ is an ideal, $a \in \bar{A}$ and $r \in R$, then $ra + I = (r + I)(a + I) \in (R/I)A \subseteq A$ so $ra \in \bar{A}$ and $ar + I = (a + I)(r + I) \in A(R/I) \subseteq A$ so $ar \in \bar{A}$. Thus if $A$ is an ideal in $R/I$ then $\bar{A}$ is an ideal in $R$. Conversely, if $\bar{A}$ is an ideal in $R$ and if $a + I \in A, r + I \in R/I$ then $a \in \bar{A}$ and so $ra, ar \in \bar{A}$. Then $(r + I)(a + I) = ra + I \in A$ and $(a + I)(r + I) = ar + I \in A$ so $A$ is an ideal in $R/I$.

#11 Let $G$ be a group and $N$ a normal subgroup of $G$. Prove that every subgroup of $G/N$ has the form $H/N$ where $H$ is a subgroup of $G$ which contains $N$. Also show that $H$ is a normal subgroup of $G$ if and only if $H/N$ is a normal subgroup of $G/N$.

**Solution:** This is parallel to the solution of #10. Let $K$ be a subgroup of $G/N$. Define $\bar{K} = \{g \in G | gN \in K\}$. Let $g_1, g_2 \in \bar{K}$. Then $g_1g_2N = (g_1N)(g_2N) \in K$ and $g_1^{-1}N = (g_1N)^{-1} \in K$.Thus $g_1g_2, g_1^{-1} \in \bar{K}$ so $\bar{K}$ is a subgroup of $G$. Now if $h \in N$ we have $hN = N = e_{G/N} \in K$. Thus $h \in \bar{K}$ and so $N \subseteq \bar{K}$. Then $N$ is a normal subgroup of $\bar{K}$ and $\bar{K}/N = \{gN | g \in \bar{K}\} = K$. Furthermore, if $K$ is a normal subgroup in $G/N, h \in \bar{K}$ and $g \in G$, then $ghg^{-1}N = (gN)(hN)(gN)^{-1} \in K$ so $ghg^{-1} \in \bar{K}$ Thus if $K$ is a normal subgroup of $G/N$ then $\bar{K}$ is a normal subgroup of $G$. Conversely, if $\bar{K}$ is a normal subgroup of $G$ and if $hN \in K, gN \in G/N$ then $h \in \bar{K}$ and so $ghg^{-1} \in \bar{K}$. Then $(gN)(hN)(gN)^{-1} = ghg^{-1}N \in K$ so $K$ is a normal subgroup of $G/N$.

#12 Let $G$ and $H$ be groups, $N$ be a normal subgroup of $G$, and $f$ be a homomorphism from $G$ to $H$.

(a) Let $e_G$ be the identity element of $G$, $e_H$ be the identity element of $H$, and let $g \in G$. Show that $f(e_G) = e_H$ and that $f(g^{-1}) = f(g)^{-1}$.

(b) Show that $ker(f)$ is a normal subgroup of $G$.

(c) Show that $f(G)$ is a subgroup of $H$.

(d) Give an example to show that $f(N)$ does not have to be a normal subgroup of $H$.

(e) Show that if $f$ is surjective then $f(N)$ is a normal subgroup of $f(G)$.

**Solution:**

(a) $f(e_G) = f(e_Ge_G) = f(e_G)f(e_G)$ and so

$$e_H = f(e_G)(f(e_G))^{-1} = f(e_G)f(e_G)(e(e_G)^{-1} = f(e_G).$$

Then $e_H = f(e_G) = f(gg^{-1}) = f(g)f(g^{-1})$ and so

$$f(g)^{-1} = f(g)^{-1}e_H = f(g)^{-1}f(g)f(g)^{-1} = f(g)^{-1}.$$

(b) Let $g_1, g_2 \in ker(f)$ and $h \in G$. Then $f(g_1g_2) = f(g_1)f(g_2) = e_He_H = e_H$ so $g_1, g_2 \in ker(f)$ and $f(g_1^{-1}) = f(g_1)^{-1} = e_H^{-1} = e_H$ so $g_1^{-1} \in ker(f)$. Hence $ker(f)$ is a subgroup of $G$. Also $f(hg_1h^{-1}) = f(h)f(g_1)f(h)^{-1}$. Since $g_1 \in ker(f)$ this is equal to $f(h)e_Hf(h)^{-1} = f(h)f(h)^{-1} = e_H$. Thus $hg_1h^{-1} \in ker(f)$ and so $ker(f)$ is a normal subgroup of $G$.

(c) Let $u_1, u_2 \in f(G)$. Then $u_1 = f(g_1)$ and $u_2 = f(g_2)$ for some $g_1, g_2 \in G$. Then $u_1u_2 = f(g_1)f(g_2) = f(g_1g_2) \in f(G)$. Also $u_1^{-1} = f(g_1)^{-1} = f(g_1^{-1}) \in f(G)$. Thus $f(G)$ is a sbugroup of $H$.

(d) Let $G$ be a cyclic group of order 2 generated by an element $a$. Thus $G = \{e_G, a\}$. Let $H = S_3$. Define $f : G \to H$ by $f(a) = (12), f(e_G) = e_H = (1)(2)(3)$. Then $f$ is a homomorphism and $f(G) = \{(1)(2)(3), (12)\}$. Then $f(G)$ is not normal in $H$, since $(13)(12)(13)^{-1} = (13)(12)(13) = (23) \notin f(G)$.

(e) We know (from part (c)) that $f(N)$ is a subgroup of $H$. Let $u \in f(N)$ and $h \in H$. Then $u = f(v)$ for some $v \in N$ and (since $f$ is surjective) $h = f(g)$ for some

$g \in G$. Then $huh^{-1} = f(g)f(v)f(g)^{-1} = f(g)f(v)f(g^{-1}) = f(gvg^{-1})$. Since $N$ is normal in $G, gvg^{-1} \in N$ and so $huh^{-1} \in f(N)$. Thus $f(N)$ is normal in $H$.

#13 Write (137562)(234)(57) as a product of disjoint cycles.

**Solution:** (134)(276)

#14 (a) Find $\sigma \in S_8$ such that $\sigma(87654321) = (12345678)$.
(b) Find $\tau \in S_8$ such that $\tau(87654321)\tau^{-1} = (12345678)$.

**Solution:**
(a) $\sigma = (12345678)(87654321)^{-1} = (12345678)(12345678) = (1357)2468)$.
(b) $\tau(87654321)\tau^{-1} = (\tau(8)\tau(7)...\tau(1))$ and so we may take

$$\tau(8) = 1, \tau(7) = 2, ..., \tau(1) = 8.$$

Thus $\tau = (18)(27)(36)(45)$ satisfies the conditions. (There are 7 other possibilities for $\tau$.)

#15 Let $C(n)$ denote the cyclic group of order $n$.
(a) Show that $C(5) \times C(6)$ is isomorphic to $C(30)$.
(b) Show that $C(2) \times C(8)$ is not isomorphic to $C(8)$

**Solution:**
(a) Let $< a >$ and $< b >$ be cyclic groups where $a$ has order 5 and $b$ has order 6. Then $< a > \times < b >= \{(a^i, b^j)|0 \leq i < 5, 0 \leq j < 6\}$. Suppose $(a, b)^k = (e, e)$. Since $(a, b)^k = (a^k, b^k)$ we have $a^k = e$ and $b_k = e$. Thus $5|k$ and $6|k$. Hence 30 divides $k$ and so $(a, b)$ has order 30. But $| < a > \times < b > | = 30$ so $< a > \times < b >=< (a, b) >$ is cyclic of order 30.
(b) $C(2) \times C(8)$ has order 16 while $C(8)$ has order 8, so they cannot be isomorphic.

#16 (a) Can $S_{10}$ contain an element of order 14? Why or why not?
(b) Can $S_{10}$ contain an element of order 16? Why or why not?

**Solution:**
(a) Yes. (1234567)(89) is such an element.
(b) No. Suppose $\sigma \in S_{10}$ has order 16. Since $\sigma$ a product of disjoint cycles, since a cycle of length $k$ has order $k$, and since disjoint cycles commute, we see that the length of any cycle occuring in the expression for $\sigma$ must be a divisor of 16, hence must be $1, 2, 4$ or 8. But then $\sigma^8$ is the identity, so the order of $\sigma$ is a divisor of 8.

#17 Let $G$ be a group, $H$ be a subgroup of $G$, ad $a, b \in G$.
(a) Show that either $Ha = Hb$ or $Ha \cap Hb = \emptyset$.
(b) Show that $|Ha| = |Hb|$.
(c) Suppose $|G|$ is finite. Prove that $|H|$ divides $|G|$.

**Solution:**
(a) Suppose $c \in Ha \cap Hb$. Then $c = h_1 a = h_2 b$ for some $h_1, h_2 \in H$. Hence $a = h_1^{-1}h_1 a = h_1^{-1}h_2 b$ and so $ab^{-1} = h_1^{-1}h_2 bb^{-1} = h_1^{-1}h_2 \in H$. Also $ba^{-1} = (ab^{-1})^{-1} \in H$.

Then if $u \in Ha$ we have $u = ka$ for some $k \in H$ and so $u = kab^{-1}b$. But $kab^{-1} \in H$ and so $u \in Hb$. Thus $Ha \subseteq Hb$. Similarly, if $v \in Hb$ then $v = lb$ for some $l \in H$ and $v = lba^{-1}a$. Since $lba^{-1} \in H$ we have $v \in Ha$ and so $Hb \subseteq Ha$. Thus $Ha = Hb$.

(b) Define $f : Ha \to Hb$ and $g : Hb \to Ha$ by $f(u) = ua^{-1}b$ and $g(v) = vb^{-1}a$. Then $f$ and $g$ are inverse mappings, so both are one-to-one and onto. Therefore $|Ha| = |Hb|$.

(c) In view of (a) $G$ is the union of the distinct right coset of $H$. The number of distinct right cosets of $H$ in $G$ is usually denoted $[G : H]$. Since these all contain $|H|$ elements, we have $|G| = [G : H]|H|$.

#18 (a) Let $R = \mathbf{Z}[\sqrt{7}]$. Show that the quotient field of $R$ is isomorphic to $\mathbf{Q}[\sqrt{7}]$.

(b) Prove that $\mathbf{Q}[\sqrt{7}]$ is a Euclidean domain with $\delta(a + b\sqrt{7}) = a^2 + 7b^2$.

**Solution:**

(a) Let $0 \neq u = a + b\sqrt{7} \in \mathbf{Q}[\sqrt{7}]$. Then $u(a - b\sqrt{7}) = a^2 - 7b^2$. Since $\sqrt{7}$ is irrational, this is $\neq 0$. Thus $u((a - b\sqrt{7})(a^2 - 7b^2)^{-1} = 1$. Hence every nonzero element of $\mathbf{Q}[\sqrt{7}]$ has an inverse and so $\mathbf{Q}[\sqrt{7}]$ is a field.

Now let $\mathbf{Z}[\sqrt{7}] \subseteq F \subseteq \mathbf{Q}[\sqrt{7}]$ where $F$ is a field. Then $\sqrt{7} \in F$. Furthermore, $\mathbf{Z} \subseteq F$ and since $F$ is a field, this means $\mathbf{Q} \subseteq F$. Thus $F = \mathbf{Q}[\sqrt{7}]$. Since any field containing $\mathbf{Z}[\sqrt{7}]$ contains subfield isomorphic to the quotient field, $\mathbf{Q}[\sqrt{7}]$ must be isomorphic to the quotient field.

(b) Since $\mathbf{Q}[\sqrt{7}]$ is a field, it is a Euclidean domain for any function $\delta$, in particular for the given function.

#19 Let $G$ be a group and $H, K$ be subgroups of $G$. Assume $HK = KH$.

(a) Show that $HK$ is a subgroup of $G$.

(b) Is $H$ a normal subgroup of $HK$? (Think about subgroups of $S_3$.)

(c) Suppose $H \cap K = \{e\}$ and $hk = kh$ for all $h \in H, k \in K$. Prove that $HK$ is isomorphic to $H \times K$.

**Solution:**

(a) Let $u_1, u_2 \in HK$. Then $u_1 = h_1k_1, u_2 = h_2k_2$ for some $h_1, h_2 \in H, k_1, k_2 \in K$. Then $u_1u_2 = (h_1k_1)(h_2k_2) = h_1(k_1h_2)k_2$. Since $HK = KH$ there are some $h_3 \in H, k_3 \in K$ so that $k_1h_2 = h_3k_3$. Then $u_1u_2 = h_1(k_1h_2)k_2 = h_1(h_3k_3)k_2 = (h_1h_3)(k_3k_2) \in HK$. Also $u_1^{-1} = (h_1k_1)^{-1} = k_1^{-1}h^{-1} \in KH = HK$. Thus $HK$ is a subgroup of $G$.

(b) $H$ is not necessarily normal in $HK$. For example if $H = \{id, (12)\} \subseteq S_3$ and $K = \{id, (123), (132)\} \subseteq S_3$ then $HK = KH = S_3$ but we know that $H$ is not a normal subgroup of $S_3$ (for $(13)(12)(13) = (23) \notin H$).

(c) Define $f : H \times K \to HK$ by $f((h, k)) = hk$. Then for $(h_1, k_1), (h_2, k_2) \in H \times K$ we have $f(((h_1, k_1)(h_2, k_2)) = f((h_1h_2, k_1k_2)) = h_1h_2k_1k_2$. Now by our assumption we have $h_2k_1 = k_1h_2$ so $f((h_1, k_1)(h_2, k_2)) = h_1h_2k_1k_2 = h_1k_1h_2k_2 = f((h_1, k_1))f((h_2, k_2))$. Thus $f$ is a homomorphism. Now any element in $HK$ has the form $hk$ for some $h \in H, k \in K$. But $hk = f((h, k))$. Thus $f$ is onto. Also, if $(h, k) \in ker(f)$ then $e = f((h, k)) = hk$ so $h = k^{-1} \in H \cap K = \{e\}$. Thus $ker(f) = \{(e, e)\}$ so $f$ is one-to-one.

#20 Let $K = \{f \in \mathbf{C}[x] | f(-2) = 0\}$ and $L = \{g \in \mathbf{C}[x] | g(-2) = g(5) = 0\}$.

(a) Show that $K$ and $L$ are ideals in $\mathbf{C}[x]$.

(b) What is the quotient $\mathbf{C}[x]/K$?
(c) What is the quotient $\mathbf{C}[x]/L$?

**Solution:** Let $\theta : \mathbf{C}[x] \to \mathbf{C}$ be defined by $\theta(h(x)) = h(-2)$. Then $\theta$ is a homomorphicm and is surjective (since the constant polynomial $c$ maps to the complex number $c$). The kernel of $\theta$ is $K$. Similarly, define $\tau : \mathbf{C}[x] \to \mathbf{C} \times \mathbf{C}$ by $\tau(h(x)) = (\tau(-2), \tau(5))$. Then $\tau$ is a homomorphism and is surjective (since the polynomial $\frac{-a}{7}(x-5) + \frac{b}{7}(x+2)$ maps to the pair $(a, b)$. The kernel of $\tau$ is $L$. Now (a) follows since $K$ and $L$ are kernels of homomorphisms. By applying the First Isomorphism Theorem to $\theta$ we see that $\mathbf{C}[x]/K$ is isomorphic to $\mathbf{C}$ and by applying the First Isomorphism Theorem to $\tau$ we see that $\mathbf{C}[x]/L$ is isomorphic to $\mathbf{C} \times \mathbf{C}$.