Quiz 1

September 14, 2005

Division: **ID#:** **Name:**

1. Let R be any ring. Suppose that a, b are elements of R.

   (a) Show that $a \cdot 0 = 0$.

   (b) Show that $a \cdot (-b) = -(ab)$.

2. A ring is called *Boolean* if $r^2 := r \cdot r = r$ for all $r \in R$. If R is a Boolean ring, prove that $2r := r + r = 0$ and that R is necessarily commutative.

Message: Any requests?

Solutions to Quiz 1

September 14, 2005

1. Let R be any ring. Suppose that a, b are elements of R.

   (a) Show that $a \cdot 0 = 0$.

   Solution:

   $$0 = a \cdot 0 + (-(a \cdot 0)) = a \cdot (0 + 0) + (-(a \cdot 0)) = a \cdot 0 + a \cdot 0 + (-(a \cdot 0)) = a \cdot 0.$$

   ■

   (b) Show that $a \cdot (-b) = -(ab)$.

   Solution:

   $$a \cdot b + a \cdot (-b) = a \cdot (b + (-b)) = a \cdot 0 = 0$$

   by (a). By adding $-(a \cdot b)$ on both hand sides, we have

   $$a \cdot (-b) = -(ab).$$

   ■

2. A ring is called *Boolean* if $r^2 := r \cdot r = r$ for all $r \in R$. If R is a Boolean ring, prove that $2r := r + r = 0$ and that R is necessarily commutative.

   Solution: Let $r, s \in R$.

   $$r + s = (r + s)^2 = r^2 + r \cdot s + s \cdot r + s^2 = r + s + r \cdot s + s \cdot r.$$

   Hence by adding the additive inverse of $r + s$ to both hand sides, we obtain

   $$r \cdot s + s \cdot r = 0.$$

   By setting $r = s$, we have

   $$0 = r^2 + r^2 = r + r = 2r.$$

   Hence in particular $r \cdot s + r \cdot s = 2(r \cdot r) = 0$. So $r \cdot s = -(r \cdot s)$. Now it follows from the equation above we have $r \cdot s = s \cdot r$.

   Thus R is commutative. ■

Quiz 2

September 26

Division: **ID#:** **Name:**

1. Let I be a two-sided ideal of a ring R. For x, x', y and $y' \in R$ show that the following holds.

$$(x + I = x' + I) \wedge (y + I = y' + I) \Rightarrow xy + I = x'y' + I.$$

2. Let $\theta : R \to S$ be a ring homomorphism, and J a two-sided ideal of S. Show that $\theta^{-1}(J) = \{x \in R \mid \theta(x) \in J\}$ is a two-sided ideal of R.

Message: Requests? Questions?

Solutions to Quiz 2

September 26, 2005

1. Let I be a two-sided ideal of a ring R. For x, x', y and $y' \in R$ show that the following holds.

$$(x + I = x' + I) \wedge (y + I = y' + I) \Rightarrow xy + I = x'y' + I.$$

Solution: First recall that if H is a subgroup of a group G. Then $aH = bH$ if and only if $a^{-1}b \in H$. Hence $x + I = x' + I$ if and only if $-x + x' \in I$. That is there is an element $a \in I$ such that $x' = x + a$. Similarly there is an element $b \in I$ such that $y' = y + b$. Since I is a two-sided ideal, $xb \in I$ and $ay \in I$. So

$$-xy + x'y' = -xy + (x + a)(y + b) = xb + ay \in I.$$

Hence $xy + I = x'y' + I$ as desired. ∎

2. Let $\theta : R \to S$ be a ring homomorphism, and J a two-sided ideal of S. Show that $\theta^{-1}(J) = \{x \in R \mid \theta(x) \in J\}$ is a two-sided ideal of R.

Solution: Let x, $y \in \theta^{-1}(J)$, and $r \in R$. Then $\theta(x) \in J$, $\theta(y) \in J$ and $\theta(r) \in S$. Hence we have

$$\begin{aligned} \theta(x + y) &= \theta(x) + \theta(y) \in J, \text{ so } x + y \in \theta^{-1}(J) \\ \theta(rx) &= \theta(r)\theta(x) \in J, \text{ so } rx \in \theta^{-1}(J) \\ \theta(xr) &= \theta(x)\theta(r) \in J, \text{ so } xr \in \theta^{-1}(J) \end{aligned}$$

Therefore $\theta^{-1}(\theta)$ is a two-sided ideal. ∎

Quiz 3

October 3, 2005

Division: **ID#:** **Name:**

1. Prove that a finite integral domain is a field.

2. Let x, y and z be integers. Suppose $6z^2 = x^2 + y^2$. Show that $x = y = z = 0$.

Message: Requests? Questions?

Solutions to Quiz 3

1. Prove that a finite integral domain is a field.

   Solution: Let R be a finite integral domain. Since an integral domain is a commutative ring with identity, it suffices to show that every nonzero element has its (multiplicative) inverse. Let a be a nonzero element of R. Let ℓ_a is a mapping defined by:

   $$\ell_a : R \longrightarrow R \ (x \mapsto ax).$$

   Then ℓ_a is an injection. In fact if $\ell_a(x) = \ell_a(y)$, then $ax = ay$ or $a(x - y) = 0$. Since $a \neq 0$ and R is an integral domain, $x - y = 0$. Hence $x = y$. Thus ℓ_a is an injection.

   Since R is finite, ℓ_a is surjective as well. Hence there is an element $b \in R$ such that $\ell_a(b) = 1$, and $ab = 1$. Since R is commutative, $ab = ba = 1$ and b is an inverse of a. Therefore R is a field. ■

2. Let x, y and z be integers. Suppose $6z^2 = x^2 + y^2$. Show that $x = y = z = 0$.

   Solution: Suppose at least one of x, y and z is nonzero. Choose x, y and z so that $\max\{|x|, |y|, |z|\}$ is minimum. Suppose there is a common divisor $d > 1$. Let $x = dx_1$, $y = dy_1$ and $z = dz_1$. Then

   $$6d^2z_1^2 = d^2x_1^2 + d^2y_1^2 = d^2(x_1^2 + y_1^2).$$

   By dividing through d^2, we have $6z_1^2 = x_1^2 + y_1^2$. This contradicts the minimality of $\max\{|x|, |y|, |z|\}$. Hence x, y and z are coprime.

   Now we consider in $\boldsymbol{Z}_3 = \{[0], [1], [2]\}$. Note that

   $$[x]^2, \ [y]^2 \in \{[0]^2, [1]^2, [2]^2\} = \{[0], [1]\}.$$

   On the other hand,

   $$[0] = [6][z]^2 = [6z^2] = [x^2 + y^2] = [x]^2 + [y]^2.$$

   Hence the only possibility is that $[x] = [y] = [0]$. So x and y are divisible by 3. Since $6z^2 = x^2 + y^2$, $6z^2$ is divisible by 9 and z^2 is divisible by 3. Thus 3 is a common divisor of x, y and z. This is a contradiction. ■

Take-Home Midterm *Due: 9:00 a.m. October 12, 2005*

Division: **ID#:** **Name:**

1. Let R be a ring with identity element. Prove or find a counter example for the following statements.

   (a) For a, $b \in R$, $(-a)(-b) = ab$, where $-a$ and $-b$ are additive inverses of a and b respectively.

   (b) For a, b and $c \in R$ with $c \neq 0$, $ac = bc$ implies $a = b$.

   (c) If there are elements a, $b \in R$ such that $ab = 1$, then the element b is not a left zero divisor.

   (d) Let f and g be polynomials in $R[t]$. Then $\deg(f) + \deg(g) = \deg(fg)$.

2. Let R be a ring with identity such that $Ra = R$ for every nonzero element $a \in R$. Show that R is a division ring. (R may not be commutative.)

3. Let I and J be two-sided ideals of a commutative ring R with identity.

   (a) Show that IJ is a two-sided ideal contained in $I \cap J$. Recall that IJ consists of sums of products of elements of I and J, i.e., elements of the form $\sum_i a_i b_i$, where $a_i \in I$, $b_i \in J$.

   (b) Show that if $I + J = R$, then $IJ = I \cap J$.

4. Let $\boldsymbol{Q}[t]$ be a polynomial ring over $\boldsymbol{Q}$ and $R = \{f(\sqrt{-5}) \mid f(t) \in \boldsymbol{Q}[t]\}$.

   (a) Show that $R = \{a + b\sqrt{-5} \mid a,\ b \in \boldsymbol{Q}\}$, and R is a field.

   (b) $\boldsymbol{Q}[t](t^2 + 5)$ is a maximal ideal of $\boldsymbol{Q}[t]$.

5. Let p be an odd prime number. If an equation $pz^2 = x^2 + y^2$ has solutions x, y and $z \in \boldsymbol{Z}$ such that $(x, y, z) \neq (0, 0, 0)$, then 4 divides $p - 1$. (Hint: First prove that 4 divides $p - 1$ if and only if $[-1]_p$ is a square of an element in $\boldsymbol{Z}_p$.)

Message: Requests? Questions?

Solutions to Midterm

October 15, 2005

1. Let R be a ring with identity element. Prove or find a counter example for the following statements.

   (a) For $a, b \in R$, $(-a)(-b) = ab$, where $-a$ and $-b$ are additive inverses of a and b respectively.

   Solution: For all $a \in R$, $0 = a0 + (-a0) = a(0+0) + (-a0) = a0 + a0 + (-a0) = a0 + 0 = a0$. Hence $a0 = 0$. Similarly, $0a = 0$ for all $a \in R$.

$$\begin{aligned}(-a)(-b) + (-ab) &= (-a)(-b) + 0b + (-ab) \\ &= (-a)(-b) + ((-a)+a)b + (-ab) = (-a)(-b) + (-a)b + ab + (-ab) \\ &= (-a)((-b)+b) + 0 = (-a)0 = 0.\end{aligned}$$

   Hence $(-a)(-b)$ is the additive inverse of $-ab$, which is ab. ■

   (b) For a, b and $c \in R$ with $c \neq 0$, $ac = bc$ implies $a = b$.

   Solution: Let $R = \boldsymbol{Z}_4 = \{[0],[1],[2],[3]\}$, and $a = [2]$, $b = [0]$, $c = [2]$. Then $ac = bc = [0]$, while $a \neq b$. ■

   (c) If there are elements $a, b \in R$ such that $ab = 1$, then the element b is not a left zero divisor.

   Solution: Let $c \in R$ be an element satisfying $bc = 0$. Then

$$c = 1c = (ab)c = a(bc) = a0 = 0.$$

   Hence $c = 0$. Therefore b cannot be a left zero divisor. ■

   (d) Let f and g be polynomials in $R[t]$. Then $\deg(f) + \deg(g) = \deg(fg)$.

   Solution: Let $R = \boldsymbol{Z}_4$ and $f = g = [2]$. Then $\deg(f) = \deg(g) = 0$ and $\deg(fg) = \deg(0) = -\infty$. Hence $\deg(f) + \deg(g) \neq \deg(fg)$ in this case. ■

2. Let R be a ring with identity such that $Ra = R$ for every nonzero element $a \in R$. Show that R is a division ring. (R may not be commutative.)

   Solution: Let a be a nonzero element of R. It suffices to show that a has a multiplicative inverse. If $1 = 0$, $a = a1 = a0 = 0$ and $R = \{0\}$. Hence we may assume that $1 \neq 0$. Since $1 \in R = Ra$ by assumption, there exists $b \in R$ such that $1 = ba$. Since $1 \neq 0$, $b \neq 0$. By assumption, $1 \in R = Rb$ and there exists $c \in R$ such that $1 = cb$. Now $a = 1a = (cb)a = c(ba) = c1 = c$. Hence $1 = cb = ab$. Since $ba = 1$, b is a multilicative inverse of a. ■

3. Let I and J be two-sided ideals of a commutative ring R with identity.

   (a) Show that IJ is a two-sided ideal contained in $I \cap J$. Recall that IJ consists of sums of products of elements of I and J, i.e., elements of the form $\sum_i a_i b_i$, where $a_i \in I$, $b_i \in J$.

   Solution: Let $x \in IJ$ and $y \in IJ$. Then by the definition of IJ, there exist a_i, $a'_j \in I$ and b_i, $b'_j \in J$ such that $x = \sum_i a_i b_i$, $y = \sum_j a'_j b'_j$. Suppose $r, s \in R$.

Then

$$\begin{aligned} x+y &= \sum_i a_ib_i + \sum_j a'_jb'_j \in IJ \\ rx &= r\sum_i a_ib_i = \sum_i (ra_i)b_i \in IJ \end{aligned}$$

Hence IJ is a two-sided ideal. Since both I and J are two-sided ideals, $a_ib_i \in I \cap J$ for each i and $x = \sum_i a_ib_i \in I \cap J$. Therefore $IJ \subseteq I \cap J$. ■

(b) Show that if $I + J = R$, then $IJ = I \cap J$.

Solution: Since $IJ \subseteq I \cap J$, it suffices to show that $I \cap J \subseteq IJ$. Since $1 \in R = I + J$, there exist $a \in I$ and $b \in J$ such that $1 = a + b$. Let $x \in I \cap J$. Then

$$x = 1x = (a+b)x = ax + bx = ax + xb \in IJ.$$

Note that $x \in J$ implies $ax \in IJ$ and $x \in I$ implies $xb \in IJ$. Therefore $I \cap J \subseteq IJ$ and $IJ = I \cap J$. ■

4. Let $\boldsymbol{Q}[t]$ be a polynomial ring over $\boldsymbol{Q}$ and $R = \{f(\sqrt{-5}) \mid f(t) \in \boldsymbol{Q}[t]\}$.

(a) Show that $R = \{a + b\sqrt{-5} \mid a,\ b \in \boldsymbol{Q}\}$, and R is a field.

Solution: Let $\phi : \boldsymbol{Q}[t] \to \boldsymbol{C}$, $(f(t) \mapsto f(\sqrt{-5}))$, where $\boldsymbol{C}$ denote the complex number field. Since $(\sqrt{-5})^2 = -5 \in \boldsymbol{Q}$, $\mathrm{Im}(\phi) \subseteq R$. Since $f(a+bt) = a+b\sqrt{-5}$, $\mathrm{Im}(\phi) = R$. Clearly ϕ is a ring homomorphism. Since the image of a ring homomorphism is a subring, R is a ring. If $a + b\sqrt{-5} \in R$ is a nonzero element, $a \neq 0$ or $b \neq 0$ and $(a - b\sqrt{-5})/(a^2 + 5b^2)$ is an inverse of $a + b\sqrt{-5}$. Hence R is a field. ■

(b) $\boldsymbol{Q}[t](t^2 + 5)$ is a maximal ideal of $\boldsymbol{Q}[t]$.

Solution: Let $I = \boldsymbol{Q}[t](t^2 + 5)$. By construction, it is an ideal of $\boldsymbol{Q}[t]$. Since $t^2 + 5 \in \mathrm{Ker}(\phi)$ and $\mathrm{Ker}(\phi)$ is an ideal, $I \subseteq \mathrm{Ker}(\phi)$. Let $f(t) \in \mathrm{Ker}(\phi)$. Then there exists $q(t) \in \boldsymbol{Q}[t]$ such that $f(t) = q(t)(t^2+5) + bt + a$ for some $a,\ b \in \boldsymbol{Q}$. Since $f(t) \in \mathrm{Ker}(\phi)$, $0 = f(\sqrt{-5}) = a + b\sqrt{-5}$. Therefore $a = b = 0$. (To see this fact, for example take a product with $a - b\sqrt{-5}$ to get $a^2 + 5b^2 = 0$.) So $f(t) = q(t)(t^2 + 5) \in I$. Therefore $I = \mathrm{Ker}(\phi)$. By an isomorphism theorem, $\boldsymbol{Q}[t]/I \simeq R$. Since R is a field, I is a maximal ideal. ■

5. Let p be an odd prime number. If an equation $pz^2 = x^2 + y^2$ has solutions x, y and $z \in \boldsymbol{Z}$ such that $(x, y, z) \neq (0, 0, 0)$, then 4 divides $p - 1$. (Hint: First prove that 4 divides $p - 1$ if and only if $[-1]_p$ is a square of an element in $\boldsymbol{Z}_p$.)

Solution: First we show that if $[-1]$ is a square of an element in $\boldsymbol{Z}_p$, then $p-1$ is divisible by 4. Suppose $[a]^2 = [-1]$. Then the order of $[a]$ in $\boldsymbol{Z}_p^*$ is of order 4. Hence $4 = |\langle [a] \rangle|$ divides the order $p - 1$ of $\boldsymbol{Z}_p^*$.

Suppose the equation $pz^2 = x^2+y^2$ has solutions x, y and $z \in \boldsymbol{Z}$ such that $(x, y, z) \neq (0, 0, 0)$. Suppose both x and y are divisible by p. Then p^2 divides pz^2 and z is divisible by p. And $(x/p, y/p, z/p)$ is a soluton to the equation. So after dividing x, y and z through by a power of p, we may assume that either x or y is not divisible by p. Then in $\boldsymbol{Z}_p$, $[x]^2 + [y]^2 = 0$ and $[x] \neq 0$ or $[y] \neq 0$. Suppose $[x] \neq 0$. Then $[-1] = ([y][x]^{-1})^2$, and $[-1]$ is a square in $\boldsymbol{Z}_p$. So $p - 1$ is divisible by 4 ■

Quiz 4

October 17, 2005

Division: **ID#:** **Name:**

1. Let R be a commutative ring with identity. Prove the following.

   (a) $0 \mid a$ if and only if $a = 0$.

   (b) If $a \mid b$ and $a \mid c$, then $a \mid bx + cy$ for all $x, y \in R$.

   (c) If u is a unit, then $a \mid u$ if and only if a is a unit.

2. Let R be an integral domain, and $R[t]$ the ring of polynomials in t over R. Show that $U(R[t]) = U(R)$.

Message: : Requests? Questions?

Solutions to Quiz 4

October 17, 2005

1. Let R be a commutative ring with identity. Prove the following.

   (a) $0 \mid a$ if and only if $a = 0$.

   Solution: Suppose $0 \mid a$. Then there exists $b \in R$ such that $a = 0b$. Hence $a = 0$. Conversely, suppose $a = 0$. Then $0 = 0a$ and $0 \mid a$. ■

   (b) If $a \mid b$ and $a \mid c$, then $a \mid bx + cy$ for all x, $y \in R$.

   Solution: By assumption, there exist d, $e \in R$ such that $b = ad$, $c = ae$. Hence $bx + cy = adx + aey = a(dx + ey)$. Therefore $a \mid bx + cy$ fore all x, $y \in R$. ■

   (c) If u is a unit, then $a \mid u$ if and only if a is a unit.

   Solution: Suppose $a \mid u$. Then there exists $b \in R$ such that $u = ab$. Since u is a unit, $1 = abu^{-1}$. Thus a is a unit with bu^{-1} as its inverse. Note that R is commutative. Conversely if a is a unit. Then $u = a(a^{-1})u$, and $a \mid u$. ■

2. Let R be an integral domain, and $R[t]$ the ring of polynomials in t over R. Show that $U(R[t]) = U(R)$.

   Solution: Let f, $g \in R[t]$ such that $f \cdot g = 1$. Then $f \neq 0$ and $g \neq 0$. In particular $\deg(f), \deg(g) \geq 0$. Since R is an integral domain, the formula $\deg(f \cdot g) = \deg(f) + \deg(g)$ holds. Since $0 = \deg(1) = \deg(f \cdot g)$ and $\deg(f)$, $\deg(g) \geq 0$, we have $\deg(f) = \deg(g) = 0$ and f, $g \in R$. Since $f \cdot g = 1$, f, $g \in U(R)$. The other includion $U(R) \subseteq U(R[t])$ is clear. Therefore $U(R[t]) = U(R)$ ■

Quiz 5

October 26, 2005

Division: **ID#:** **Name:**

Let a, b be elements in a domain R. A *greatest common divisor* of a and b is a ring element d such that (i) $d \mid a$ and $d \mid b$; (ii) if $c \mid a$ and $c \mid b$ for some $c \in R$, then $c \mid d$.

Show the following.

1. Let a and b be elements of an integral domain R. Let $I = \{ax + by \mid x, y \in R\}$. If there is an element $d \in R$ such that $I = \langle d \rangle$, then d is a greatest commond divisor of a and b.

2. If R is a principal ideal domain and $p \mid bc$ where p, b, $c \in R$ and p is irreducible, then $p \mid b$ or $p \mid c$.

Message: Requests? Questions?

Solutions to Quiz 5

May 15, 2005

Let a, b be elements in a domain R. A *greatest common divisor* of a and b is a ring element d such that (i) $d \mid a$ and $d \mid b$; (ii) if $c \mid a$ and $c \mid b$ for some $c \in R$, then $c \mid d$.

Show the following.

1. Let a and b be elements of an integral domain R. Let $I = \{ax + by \mid x, y \in R\}$. If there is an element $d \in R$ such that $I = \langle d \rangle$, then d is a greatest commond divisor of a and b.

   Solution: Recall that since R is an integral domain the following hold for $a, b \in R$:

   (i) $a \mid b \Leftrightarrow \langle b \rangle \subseteq \langle a \rangle$.

   (ii) $(a \mid b) \wedge (b \mid a) \Leftrightarrow (\exists u \in U(R))[b = ua]$.

   Since $I = \langle a \rangle + \langle b \rangle = \langle d \rangle$, $\langle a \rangle \subseteq \langle d \rangle$ and $\langle b \rangle \subseteq \langle d \rangle$. Hence by (i) above we have $d \mid a$ and $d \mid b$.

   Suppose $c \mid a$ and $c \mid b$, then $\langle a \rangle \subseteq \langle c \rangle$ and $\langle b \rangle \subseteq \langle c \rangle$. Hence

   $$\langle d \rangle = I = \langle a \rangle + \langle b \rangle \subseteq \langle c \rangle.$$

   Thus $c \mid d$. Therefore d is a greatest common divisor of a and b. ■

2. If R is a principal ideal domain and $p \mid bc$ where p, b, $c \in R$ and p is irreducible, then $p \mid b$ or $p \mid c$.

   Solution: Let $I = \{px + by \mid x, y \in R\}$. Since R is a principal ideal domain, there exists $d \in R$ such that $I = \langle d \rangle$ and d is a greatest common divisor of p and b. In particular, $d \mid p$ and there exists $e \in R$ such that $p = de$. Since p is irreducible, either $d \in U(R)$ or $e \in U(R)$. Hence either $I = R$ or $I = \langle p \rangle$. Suppose $I = \langle p \rangle$. Since $\langle b \rangle \subseteq I = \langle p \rangle$, $p \mid b$. Suppose $I = R$. Then there exist x, $y \in R$ such that $1 = px + by$. Now $c = pcx + bcy$. Since $p \mid bc$ by assumption, and $p \mid pcx$, we have $p \mid c$. Thus $p \mid b$ or $p \mid c$. ■

Quiz 6

November 2, 2005

Division: **ID#:** **Name:**

1. Let R be an integral domain. Let p be a non-zero element of R. Show that if $\langle p \rangle$ is a prime ideal, then p is irreducible.

2. Let $R = \{a + b\sqrt{-5} \mid a,\ b \in \boldsymbol{Z}\}$. For $\alpha = a + b\sqrt{-5}$, let $N(\alpha) = \alpha\overline{\alpha} = (a + b\sqrt{-5})(a - \sqrt{-5}) = a^2 + 5b^2$. You may assume that R is a subring of $\boldsymbol{C}$ and an integral domain. Note that $N(\alpha\beta) = N(\alpha)N(\beta)$ for $\alpha,\ \beta \in R$.

   (a) Show that for $\alpha = a + b\sqrt{-5} \in R$,
   $$\alpha \in U(R) \Leftrightarrow N(\alpha) = 1 \Leftrightarrow \alpha \in \{1, -1\}.$$

   (b) Show that 2 is an irreducible element in R.

Message: Requests? Questions?

Solutions to Quiz 6

November 2, 2005

1. Let R be an integral domain. Let p be a non-zero element of R. Show that if $\langle p \rangle$ is a prime ideal, then p is irreducible.

   Solution: Suppose $p = ab$ for some $a, b \in R$. Clearly a and b are non-zero, $a \mid p$ and $b \mid p$. Since $\langle p \rangle$ is a prime ideal and $ab = p \in \langle p \rangle$, either $a \in \langle p \rangle$ or $b \in \langle p \rangle$. These imply $p \mid a$ or $p \mid b$ respectively. Since $a \mid p$ and $b \mid p$, $p = au$ or $p = bv$ for some $u, v \in U(R)$. If $p = au$ then $0 = a(u - b)$. Since $a \neq 0$, $b = u$ is a unit. If $p = bv$, then $a = v$ is a unit. Therefore p is irreducible. ■

2. Let $R = \{a + b\sqrt{-5} \mid a, b \in \boldsymbol{Z}\}$. For $\alpha = a + b\sqrt{-5}$, let $N(\alpha) = \alpha\overline{\alpha} = (a + b\sqrt{-5})(a - \sqrt{-5}) = a^2 + 5b^2$. You may assume that R is a subring of $\boldsymbol{C}$ and an integral domain. Note that $N(\alpha\beta) = N(\alpha)N(\beta)$ for $\alpha, \beta \in R$.

   (a) Show that for $\alpha = a + b\sqrt{-5} \in R$,

   $$\alpha \in U(R) \Leftrightarrow N(\alpha) = 1 \Leftrightarrow \alpha \in \{1, -1\}.$$

   Solution: Suppose $\alpha \in U(R)$. Then there exists $\beta = c + d\sqrt{-5} \in R$ such that $\alpha\beta = 1$. Since $1 = N(1) = N(\alpha\beta) = N(\alpha)N(\beta)$ and both $N(\alpha)$ and $N(\beta)$ are non-negative integers, $N(\alpha) = 1$. Since $N(\alpha) = a^2 + 5b^2$, $N(\alpha) = 1$ if and only if $\alpha = \pm 1$. It is clear that $\{1, -1\} \subset U(R)$. ■

   (b) Show that 2 is an irreducible element in R.

   Solution: Suppose $2 = \alpha\beta$, where $\alpha, \beta \in R$. Then $4 = N(2) = N(\alpha\beta) = N(\alpha)N(\beta)$. If $\alpha \notin U(R)$ and $\beta \notin U(R)$, then $N(\alpha) = 2$ as it is a non-negative integer. Since $N(\alpha) = a^2 + 5b^2$ and 2 cannot be expressed in this form, this is impossible. Therefore either $\alpha \in U(R)$ or $\beta \in U(R)$. ■

Quiz 7

November 14, 2005

Division: **ID#:** **Name:**

In the following you may use the following fact:

If R is a UFD and $p \mid bc$ where $p, b, c \in R$ and p is irreducible, then $p \mid b$ or $p \mid c$.

1. Prove Eisenstain's Criterion:

   Let R be a unique factorization domain and let $f = a_0 + a_1 t + \cdots + a_n t^n$ be a polynomial over R. Suppose that there is an irreducible element p of R such that $p \mid a_0$, $p \mid a_1, \ldots, p \mid a_{n-1}$, but $p \nmid a_n$ and $p^2 \nmid a_0$. Then f is irreducible over R.

2. Apply Eisenstein's Criterion to prove that $2t^5 - 3t + 15$ is irreducible over $\boldsymbol{Z}$.

3. Prove that $t^4 + t^3 + t^2 + t + 1$ is irreducible over $\boldsymbol{Z}$.

Message: Requests? Questions?

Solutions to Quiz 7

November 14, 2005

In the following you may use the following fact:
If R is a UFD and $p \mid bc$ where $p, b, c \in R$ and p is irreducible, then $p \mid b$ or $p \mid c$.

1. Prove Eisenstain's Criterion:

   Let R be a unique factorization domain and let $f = a_0 + a_1 t + \cdots + a_n t^n$ be a polynomial over R. Suppose that there is an irreducible element p of R such that $p \mid a_0$, $p \mid a_1, \ldots, p \mid a_{n-1}$, but $p \nmid a_n$ and $p^2 \nmid a_0$. Then f is irreducible over R.

   See Page 132 in the textbook.

2. Apply Eisenstein's Criterion to prove that $2t^5 - 3t + 15$ is irreducible over $\boldsymbol{Z}$.

   Solution: Since $\boldsymbol{Z}$ is a ED, it is a PID, and so is a UFD. Hence we can apply Eisenstein's Criterion. Take $p = 3$ as an irreducible element in Eisenstein's Criterion. Then

$$3 \mid 15 = a_0,\ 3 \mid -3 = a_1,\ 3 \mid 0 = a_2 = a_3 = a_4,\ 3 \nmid 2 = a_5,\ 9 \nmid 15 = a_0.$$

   Hence the polynomial $2t^5 - 3t + 15$ is irreducible over $\boldsymbol{Z}$. If we apply Gauss' Lemma, we know that $2t^5 - 3t + 15$ is irreducible over $\boldsymbol{Q}$.

3. Prove that $t^4 + t^3 + t^2 + t + 1$ is irreducible over $\boldsymbol{Z}$.

   Solution: Let $f(t) = t^4 + t^3 + t^2 + t + 1$ and $g(t) = f(t+1)$. Then

$$\begin{aligned} g(t) &= (t+1)^4 + (t+1)^3 + (t+1)^2 + (t+1) + 1 = \frac{(t+1)^5 - 1}{t} \\ &= t^4 + \binom{5}{1} t^3 + \binom{5}{2} t^2 + \binom{5}{3} t + \binom{5}{4} \\ &= t^4 + 5t^3 + 10t^2 + 10t + 5. \end{aligned}$$

   Now apply Eisenstein's Criterion by setting $p = 5$. Then $g(t)$ is irreducible over $\boldsymbol{Z}$. Since $f(t+1) = g(t)$, $f(t)$ is irreducible as well. Note that if $f(t) = r(t)s(t)$, then $g(t) = f(t+1) = r(t+1)s(t+1)$.