Quiz 1

(*Due at 1:50 p.m. on Mon. Sept. 15, 2008*)

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

An *integral domain* is a commutative ring R with identity such that

$$ab = 0 \to a = 0 \text{ or } b = 0 \text{ for all } a, b \in R.$$

1. Show that if R is an integral domain, then the polynomial ring $R[t]$ is also an integral domain.

2. Show that if R is an integral domain, then the polynomial ring $R[t_1, t_1, \ldots, t_n]$ is also an integral domain.

Message: What do you expect for this course? Any requests?

Solutions to Quiz 1

An *integral domain* is a commutative ring R with identity such that

$$ab = 0 \to a = 0 \text{ or } b = 0 \text{ for all } a, b \in R.$$

1. Show that if R is an integral domain, then the polynomial ring $R[t]$ is also an integral domain.

   Solution. Let $f = a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0$ and $g = b_m t^m + b_{m-1} t^{m-1} + \cdots + b_1 t + b_0 \in R[t]$. We assume $f \neq 0$, $g \neq 0$ and show that $f \cdot g \neq 0$. In this case we may assume that $a_n \neq 0$ and $b_m \neq 0$. Now

   $$f \cdot g = a_n b_m t^{n+m} + (a_n b_{m-1} + a_{n-1} b_m) t^{n+m-1} + \cdots + (a_1 b_0 + a_0 b_1) t + a_0 b_0.$$

   Since R is an integral domain, and $a_n \neq 0 \neq b_m$, $a_n b_m \neq 0$. Therefore $f \cdot g \neq 0$ as desired. ■

   The above proof shows that $\deg f \cdot g = \deg f + \deg g$ when $f \neq 0$ and $f \neq 0$. But if one of f or g is zero, its degree is $-\infty$. Hence if we extend our addition of integers to $\boldsymbol{Z} \cup \{-\infty\}$ and $a + (-\infty) = (-\infty) + (-\infty) = -\infty$, then $\deg f \cdot g = \deg f + \deg g$ holds even when f or g is a zero polynomial. Note that zero polynomial is the only polynomial with non-integral degree and polynomials of degree zero are nonzero constants.

2. Show that if R is an integral domain, then the polynomial ring $R[t_1, t_1, \ldots, t_n]$ is also an integral domain.

   Solution. Note that $R[t_1, t_2, \ldots, t_n] = R[t_1, t_2, \ldots, t_{n-1}][t_n]$ if $n \geq 2$. So if $f \in R[t_1, t_2, \ldots, t_n]$, then f can be written as

   $$f = f_m t_n^m + f_{m-1} t_n^{m-1} + \cdots + f_1 t_n + f_0, \text{ where } f_m, f_{m-1}, \ldots, f_1, f_0 \in R[t_1, t_2, \ldots, t_{n-1}].$$

   We proceed by induction. If $n = 1$, $R[t_1]$ is an integral domain by 1. Suppose $R[t_1, t_2, \ldots, t_{n-1}]$ is an integral domain. Then by 1 $R[t_1, t_2, \ldots, t_{n-1}][t_n]$ is an integral domain as this ring is a polynomial ring over an integral domain as well. Therefore for all positive integer n, $R[t_1, t_2, \ldots, t_n]$ is an integral domain. ■

   Try a direct proof to show, say $\boldsymbol{Z}[x, y]$ is an integral domain. You will see a difficulty avoided by the proof above.

Quiz 2

(*Due at 1:50 p.m. on Mon. Sept. 22, 2008*)

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

Let R be a commutative ring with 1 and let I and J be ideals of R.

1. Show that $I + J = \{x + y \mid x \in I,\ y \in J\}$ is an ideal of R.

2. Show that with respect to entrywise addition and multiplication, $R/I \times R/J$ becomes a commutative ring with 1.

3. $\alpha : R \to R/I \times R/J$ $(x \mapsto (x + I, x + J))$ is a ring homomorphism.

4. Suppose $I + J = R$. Show that $I \cap J = IJ$, where $IJ = \{\sum_i x_i y_i \mid x_i \in I,\ y_i \in J\}$.

5. Suppose $I + J = R$. Then the homomorphism α in 3 is surjective and $R/IJ \simeq R/I \times R/J$.

Message: Please write your comments and requests.

Solutions to Quiz 2

Let R be a commutative ring with 1 and let I and J be ideals of R.

1. Show that $I + J = \{x + y \mid x \in I,\ y \in J\}$ is an ideal of R.

   Solution. Let $x, x' \in I$, $y, y' \in J$ and $r \in R$. Then

   $$(x + y) + (x' + y') = (x + x') + (y + y') \in I + J,\ -(x + y) = (-x) + (-y) \in I + J,$$

   $$\text{and } r(x + y) = rx + ry \in I + J.$$

   Hence $I + J$ is an ideal. ■

2. Show that with respect to entrywise addition and multiplication, $R/I \times R/J$ becomes a commutative ring with 1.

   Solution. Let $x, x' \in I$ and $y, y' \in J$. Binary operations are defined as follows. $(x+I, y+J)+(x'+I, y'+J) = (x+x'+I, y+y'+J)$ and $(x+I, y+J)\cdot(x'+I, y'+J) = (xx' + I, yy' + J)$. Everything is clear and $(1 + I, 1 + J)$ is the identity element of $R/I \times R/J$. ■

3. $\alpha : R \to R/I \times R/J$ $(x \mapsto (x + I, x + J))$ is a ring homomorphism.

   Solution. $\alpha(x + y) = (x + y + I, x + y + J) = (x + I, x + J) + (y + I, y + J) = \alpha(x)+\alpha(y)$ and $\alpha(x\cdot y) = (xy+I, xy+J) = (x+I, x+J)\cdot(y+I, y+J) = \alpha(x)\cdot\alpha(y)$. Hence α is a ring homomorphism. ■

4. Suppose $I + J = R$. Show that $I \cap J = IJ$, where $IJ = \{\sum_i x_i y_i \mid x_i \in I,\ y_i \in J\}$.

   Solution. Since both I and J are ideals, $IJ \subset I \cap J$. Let $x \in I \cap J$. Since $I + J = R$ and $1 \in R$, there exist $s \in I$ and $t \in J$ such that $1 = s + t$. Hence $x = x1 = x(s + t) = sx + xt \in IJ$ and $I \cap J \subset IJ$. ■

5. Suppose $I + J = R$. Then the homomorphism α in 3 is surjective and $R/IJ \simeq R/I \times R/J$.

   Solution. Let $x, y \in R$. Let s and t be those in the previous problem. In particular, $s + t = 1$ and $sy, xs \in I$, $xt, ty \in J$. Hence

   $$\begin{aligned}\alpha(xt + sy) &= (xt + sy + I, xt + sy + J) = (xt + I, sy + J)\\ &= (x(1 - s) + I, (1 - t)y + J) = (x + I, y + J).\end{aligned}$$

   Thus α is surjective. It is clear that $\ker(\alpha) = I \cap J$. Hence by the previous problem, $\ker(\alpha) = IJ$ and $R/IJ \simeq R/I \times R/J$ by the first isomorphism theorem. ■

Quiz 3

(*Due at 1:50 p.m. on Mon. Sept. 24, 2008*)

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

Let K be a field and $K[x, y]$ be a polynomial ring over K with two indeterminates x and y. Let $I = K[x, y]x + K[x, y]y = \{f(x, y) \cdot x + g(x, y) \cdot y \mid f(x, y), g(x, y) \in K[x, y]\}$.

1. Show that I is an ideal of $K[x, y]$ such that $I \neq K[x, y]$.

2. Let $\alpha : K[x, y] \to K[x, y]$ $(f(x, y) \mapsto f(x, x))$. Show that α is a ring homomorphism and $J = \ker(\alpha) = K[x, y] \cdot (x - y)$.

3. Show that J in the previous problem is a prime ideal of $K[x, y]$.

4. Show that $J \subset I$ and I is not a principal ideal.

5. Show that I is a maximal ideal of $K[x, y]$.

Message: Please write your comments and requests.

Solutions to Quiz 3

Let K be a field and $K[x, y]$ be a polynomial ring over K with two indeterminates x and y. Let $I = K[x, y]x + K[x, y]y = \{f(x, y) \cdot x + g(x, y) \cdot y \mid f(x, y), g(x, y) \in K[x, y]\}$.

1. Show that I is an ideal of $K[x, y]$ such that $I \neq K[x, y]$.

   Solution. I is clearly an ideal of $K[x, y]$. Hence its proof is omitted. Suppose $I = K[x, y]$. Then there exist $f(x, y), g(x, y) \in K[x, y]$ such that $1 = f(x, y)x + g(x, y)y$. Then $1 = f(x, 0)x \in K[x]$. By comparing the degrees in $K[x]$, we have a contradiction. Hence $I \neq K[x, y]$. ■

2. Let $\alpha : K[x, y] \to K[x, y]$ $(f(x, y) \mapsto f(x, x))$. Show that α is a ring homomorphism and $J = \ker(\alpha) = K[x, y] \cdot (x - y)$.

   Solution. It is clear that α is a ring homomorphism such that $\ker(\alpha) \supset K[x, y] \cdot (x - y)$. Let $f(x, y) \in \ker(\alpha)$ and write $f(x, y) = f_n(y)x^n + f_{n-1}(y)x^{n-1} + \cdots + f_1(y)x + f_0(y)$. Then we find $g(x, y) \in K[y][x]$ and $r(x, y) \in K[y][x]$ with $\deg_x r(x, y) < \deg_x(x - y) = 1$ such that $f(x, y) = g(x, y)(x - y) + r(x, y)$. Here $\deg_x r(x, y)$ denotes the degree of $r(x, y)$ as a polynomial in x. In particular, x does not appear in $r(x, y)$ and $r(x, y) = r_0(y)$. Since $f(x, y) \in \ker(\alpha)$, $r_0(x) = 0$ and $r(x, y) = 0$. Therefore $f(x, y) \in K[x, y] \cdot (x - y)$. ■

3. Show that J in the previous problem is a prime ideal of $K[x, y]$.

   Solution. Since the image of α is a subring of an integral domain $K[x, y]$, it is an integral domain as well. Hence its kernel is a prime ideal. ■

4. Show that $J \subset I$ and I is not a principal ideal.

   Solution. The assertion $J \subset I$ is clear. Suppose I is an principal ideal and $K[x, y] \cdot x + K[x, y] \cdot y = I = K[x, y] \cdot f(x, y)$. Since $x, y \in I$, there exist $g(x, y), h(x, y) \in K[x, y]$ such that $x = g(x, y)f(x, y)$ and $y = h(x, y)f(x, y)$. Since $0 = \deg_y x = \deg_y(g(x, y) + \deg_y f(x, y)$, $\deg_y f(x, y) = 0$. Similarly, since $0 = \deg_x y = \deg_x h(x, y) + \deg_x f(x, y)$, $\deg_x f(x, y) = 0$. Therefore $f(x, y)$ is a nonzero constant and $I = K[x, y] \cdot f(x, y) = K[x, y]$. This contradicts 1. ■

5. Show that I is a maximal ideal of $K[x, y]$.

   Solution. Let $\beta : K[x, y] \to K$ $(f(x, y) \mapsto f(0, 0))$. Then this is a surjective ring homomorphism and $\ker(\beta) \supset I$. Let $f(x, y) \in \ker(\beta)$ and $f(x, y) = f_n(y)x^n + f_{n-1}(y)x^{n-1} + \cdots + f_1(y)x + f_0(y)$. Then $f_0(0) = 0$ as $\beta(f) = 0$. Hence $f_0(y) \in K[y] \cdot y$ and $f(x, y) \in K[x, y]x + K[x, y]y = I$. ■

Quiz 4

(*Due at 1:50 p.m. on Wednesday, October 1, 2008*)

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

Let R be an integral domain. A non-constant polynomial $f(t) \in R[t]$ is said to be irreducible if $f(t) = g(t)h(t)$ for some $g(t), h(t) \in R[t]$ implies $\deg g(t) = 0$ or $\deg h(t) = 0$.

1. Let R be an integral domain. Show that $U(R[t]) = U(R)$.

2. Let $f(t) = a_0 + a_1 t + \cdots + a_n t^n \in \boldsymbol{Z}[t]$. Suppose $gcd(a_0, a_1, \ldots, a_n) = 1$, $a_n \neq 0$ and there exist $g(t), h(t) \in \boldsymbol{Q}[t]$ such that $f(t) = g(t)h(t)$. Show that there exist $g_1(t), h_1(t) \in \boldsymbol{Z}[t]$ and $c, d \in \boldsymbol{Q}$ such that $f(t) = g_1(t)h_1(t)$ and that $g_1(t) = cg(t)$ and $h_1(t) = dh(t)$. (Hint: See (7.3.6).)

3. Let $f(t) = a_0 + a_1 t + \cdots + a_n t^n \in \boldsymbol{Z}[t]$ be an irreducible polynomial in $\boldsymbol{Z}[t]$. Then $f(t)$ is irreducible in $\boldsymbol{Q}[t]$.

4. Let $f(t) = a_0 + a_1 t + \cdots + a_n t^n \in \boldsymbol{Z}[t]$. Suppose that there is a prime p such that $p \mid a_0$, $p \mid a_1, \ldots, p \mid a_{n-1}$, but p does not divide a_n and p^2 does not divide a_0. Then $f(t)$ is irreducible in $\boldsymbol{Q}[t]$. (Hint: See (7.4.9).)

Message: Please write your comments and requests.

Solutions to Quiz 4

Let R be an integral domain. A non-constant polynomial $f(t) \in R[t]$ is said to be irreducible if $f(t) = g(t)h(t)$ for some $g(t), h(t) \in R[t]$ implies $\deg g(t) = 0$ or $\deg h(t) = 0$.

1. Let R be an integral domain. Show that $U(R[t]) = U(R)$.

   Solution. Suppose $g(t)h(t) = 1$. Then $0 = \deg(g(t)h(t)) = \deg(g(t)) + \deg(h(t))$. Hence $\deg(g(t)) = \deg(h(t)) = 0$ and both $g(t)$ and $h(t)$ are constants. Therefore $g(t) \in U(R)$ and $U(R[t]) \subset U(R)$. The other inclusion is obvious. ■

2. Let $f(t) = a_0 + a_1 t + \cdots + a_n t^n \in \boldsymbol{Z}[t]$. Suppose $gcd(a_0, a_1, \ldots, a_n) = 1$, $a_n \neq 0$ and there exist $g(t), h(t) \in \boldsymbol{Q}[t]$ such that $f(t) = g(t)h(t)$. Show that there exist $g_1(t), h_1(t) \in \boldsymbol{Z}[t]$ and $c, d \in \boldsymbol{Q}$ such that $f(t) = g_1(t)h_1(t)$ and that $g_1(t) = cg(t)$ and $h_1(t) = dh(t)$. (Hint: See (7.3.6).)

   Solution. By taking the common denominators of $g(t)$ and $h(t)$, we can find $g_1(t) = b_0 + b_1 t + \cdots + b_\ell t^\ell \in \boldsymbol{Z}[t]$ and $h_1(t) = c_0 + c_1 t + \cdots + c_m t^m \in \boldsymbol{Z}[t]$ and $c, d \in \boldsymbol{Q}$ such that $g_1(t) = cg(t)$, $h_1(t) = dh(t)$ and that $ef(t) = g_1(t)h_1(t)$ for some integer $e \in \boldsymbol{Z}$. Suppose $e \neq \pm 1$. It suffices to show that each prime divisor p of e divides all coefficients of $g_1(t)$ or all coefficients of $h_1(t)$. Since $p \mid b_0 c_0 = ea_0$, we may assume that there exist indices $i > 0$ and $j \geq 0$ such that $p \mid b_0, \ldots, p \mid b_{i-1}$ and p does not divide b_i, and $p \mid c_0, \ldots, p \mid c_{j-1}$ and p does not divide c_j. Then p divides ea_{i+j} but p does not divide $b_0 c_{i+j} + \cdots + b_{i-1} c_{j+1} + b_i c_j + b_{i+1} c_{j-1} + \cdots b_{i+j} c_0$. A contradiction. ■

3. Let $f(t) = a_0 + a_1 t + \cdots + a_n t^n \in \boldsymbol{Z}[t]$ be an irreducible polynomial in $\boldsymbol{Z}[t]$. Then $f(t)$ is irreducible in $\boldsymbol{Q}[t]$.

   Solution. Let $d = gcd(a_0, a_1, \ldots, a_n)$. Then there is a polynomial $f_1(t) \in \boldsymbol{Z}[t]$ such that $f(t) = d \cdot f_1(t)$, and the greatest common divisor of the coefficients of $f_1(t)$ is 1. Hence by the previous problem, $f(t)$ is irreducible in $\boldsymbol{Q}[t]$ and hence so is $f(t)$. ■

4. Let $f(t) = a_0 + a_1 t + \cdots + a_n t^n \in \boldsymbol{Z}[t]$. Suppose that there is a prime p such that $p \mid a_0$, $p \mid a_1, \ldots, p \mid a_{n-1}$, but p does not divide a_n and p^2 does not divide a_0. Then $f(t)$ is irreducible in $\boldsymbol{Q}[t]$. (Hint: See (7.4.9).)

   Solution. Let $f(t) = g(t)h(t)$, $g(t) = b_0 + b_1 t + \cdots + b_\ell t^\ell \in \boldsymbol{Z}[t]$ and $h(t) = c_0 + c_1 t + \cdots + c_m t^m \in \boldsymbol{Z}[t]$. Since $a_0 = b_0 c_0$ is divisible by p but not p^2, there exists $i > 0$ such that $p \mid b_0, \ldots, p \mid b_{i-1}$ and p does not divide b_i, and $p \mid c_m, \ldots, p \mid c_{j+1}$ and p does not divie c_j with $j \leq m$. Since p does not divide $b_0 c_i + \cdots + b_i c_0$, $i = n$ and $h(t)$ is a constant. Therefore $f(t)$ is irreducible in $\boldsymbol{Z}[t]$. By the previous problem, it is irreducible in $\boldsymbol{Q}[t]$. ■

Quiz 5

(Due *at 1:50 p.m. on Wednesday. Oct. 8, 2008*)

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

Let $F[[t]]$ be the ring of formal power series over a field F. See Exercise (6.1.8).

1. Show that $U(F[[t]]) = \{f \in F[[t]] \mid f(0) \neq 0\}$.

2. Show that $t \cdot F[[t]]$ is the only maximal ideal in $F[[t]]$.

3. For a nonzero $f = \sum_{i=0}^{\infty} a_i t^t \in F[[t]]$, let $\delta(f)$ be the smallest index i such that $a_i \neq 0$. Show that $F[[t]]$ is Euclidean with respect to the function δ.

Message: Please write your comments and requests.

Solutions to Quiz 5

Let $F[[t]]$ be the ring of formal power series over a field F. See Exercise (6.1.8).

1. Show that $U(F[[t]]) = \{f \in F[[t]] \mid f(0) \neq 0\}$.

   Solution. Let $g = b_0 + b_1 t + \cdots$, and $fg = c_0 + c_1 t + \cdots$.

   Suppose $fg = 1$. Then $a_0 b_0 = 1$. Hence $b_0 = a_0^{-1}$. Let $i \geq 1$. Since $c_i = \sum_{j=0}^{i} a_j b_{i-j} = 0$, assuming that $b_0, b_1, \ldots, b_{i-1}$ are determined, $b_i = -a_0^{-1} \sum_{j=1}^{i} a_j b_{i-j}$. Thus the inverse is uniquely determined if $a_0 \neq 0$, and there is no inverse if $a_0 = 0$. ∎

2. Show that $t \cdot F[[t]]$ is the only maximal ideal in $F[[t]]$.

   Solution. By the previous problem, it is clear that $F[[t]] \setminus U(F[[t]]) = t \cdot F[[t]]$. Thus $t \cdot F[[t]]$ is the only maximal ideal in $F[[t]]$. Note that $F[[t]] \setminus U(F[[t]])$ is the union of all the proper ideals of $F[[t]]$. See (6.3.5). ∎

3. For a nonzero $f = \sum_{i=0}^{\infty} a_i t^t \in F[[t]]$, let $\delta(f)$ be the smallest index i such that $a_i \neq 0$. Show that $F[[t]]$ is Euclidean with respect to the function δ.

   Solution. Let $f, g \in F[[t]]$ be nonzero elements. then $\delta(fg) = \delta(f) + \delta(g) \geq \delta(f)$.

   Now let $f, g \in F[[t]]$ with $g \neq 0$. If $f = 0$, $f = 0 = 0 \cdot g + 0$ and there is nothing to prove. Suppose $\delta(f) = n$ and $\delta(g) = m$. If $n < m$, then $f = 0 \cdot g + f$ and $\delta(f) < \delta(g)$. Assume $n \geq m$. Then there exist $f_0, g_0 \in U(F[[t]])$ such that $f = f_0 \cdot t^n$ and $g = g_0 \cdot t^m$ by the first problem. Let $q = t^{n-m} \cdot g_0^{-1} \cdot f_0$. Then

   $$f - q \cdot g = f_0 \cdot t^n - t^{n-m} \cdot g_0^{-1} \cdot f_0 \cdot g_0 \cdot t^m = f_0 \cdot t^n - f_0 \cdot t^n = 0.$$

   Therefore $F[[t]]$ is an Euclidean domain. ∎

Quiz 6

(*Due at 1:50 p.m. on Wednesday. Oct. 15, 2008*)

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

Let D be an integer greater than or equal to 2. Let $R = \{a + b\sqrt{-D} \mid a, b \in \boldsymbol{Z}\}$. For $z = a + b\sqrt{-D} \in R$ let $N(z) = N(a + b\sqrt{-D}) = (a + b\sqrt{-D})(a - b\sqrt{-D}) = a^2 + b^2 D$.

1. Show that R is an integral domain but not a field.

2. Let $z, z' \in R$. Show that $N(zz') = N(z)N(z')$, and that $U(R) = \{1, -1\}$.

3. Let p be a prime number in $\boldsymbol{Z}$. If p is not irreducible in R, then there exists $z \in R$ such that $p = N(z)$. In particular, if $D \geq 3$, then 2 is an irreducible element in R.

4. Suppose $D \equiv 1 \pmod 4$. Show that both $1 + \sqrt{-D}$ and $1 - \sqrt{-D}$ are not elements in $\langle 2 \rangle$.

5. Show that if $D \equiv 1 \pmod 4$, R is not a PID. (Hint: If R is a PID, $\langle p \rangle$ is a prime ideal whenever p is an irreducible element.)

Message: Please write your comments and requests.

Solutions to Quiz 6

(*June 1, 2008*)

Let D be an integer greater than or equal to 2. Let $R = \{a + b\sqrt{-D} \mid a, b \in \boldsymbol{Z}\}$. For $z = a + b\sqrt{-D} \in R$ let $N(z) = N(a + b\sqrt{-D}) = (a + b\sqrt{-D})(a - b\sqrt{-D}) = a^2 + b^2 D$.

1. Show that R is an integral domain but not a field.

   Solution. Let $\theta : \boldsymbol{Z}[t] \to \boldsymbol{C}$ $(f(t) \mapsto f(\sqrt{-D}))$. For $f(t) \in \boldsymbol{Z}[t]$, there exist $q(t) \in \boldsymbol{Z}[t]$ and $a, b \in \boldsymbol{Z}$ such that $f(t) = q(t)(t^2 + D) + a + bt$. Since $t^2 + D \in \ker(\theta)$, $\mathrm{Im}(\theta) = R$ and R is an integral domain as it is a subring of a field $\boldsymbol{C}$. ■

2. Let $z, z' \in R$. Show that $N(zz') = N(z)N(z')$, and that $U(R) = \{1, -1\}$.

   Solution. Since $N(z) = z\overline{z}$, for $z, z' \in R$

   $$N(zz') = zz'\overline{zz'} = zz'\overline{z}\overline{z'} = z\overline{z}z'\overline{z'} = N(z)N(z').$$

   Let $z = a + b\sqrt{-D} \in R$. Suppose $N(zz') = 1$. Then $1 = N(1) = N(z)N(z')$ and $N(z) = a^2 + b^2 D$ is a nonnegative integer. Hence $N(z) = 1$ and $z = \pm 1$ as these are the only solutions of $a^2 + b^2 D = 1$, where $a, b \in \boldsymbol{Z}$. $\{1, -1\} \subset U(R)$ is clear.

3. Let p be a prime number in $\boldsymbol{Z}$. If p is not irreducible in R, then there exists $z \in R$ such that $p = N(z)$. In particular, if $D \geq 3$, then 2 is an irreducible element in R.

   Solution. Suppose p is not an irreducible element. Note that $z \in U(R)$ if and only if $N(z) = 1$. Hence if $p = zz'$ and $z, z' \notin U(R)$, then $N(z) \neq 1 \neq N(z')$. On the other hand, $p^2 = N(z)N(z')$. Since both $N(z)$ and $N(z')$ are positive integers, $N(z) = p$ as desired. Furthermore if $p = 2$, there are no $a, b \in \boldsymbol{Z}$ such that $a^2 + b^2 D = 2$ as $D \geq 3$. ■

4. Suppose $D \equiv 1 \pmod 4$. Show that both $1 + \sqrt{-D}$ and $1 - \sqrt{-D}$ are not elements in $\langle 2 \rangle$.

   Solution. Suppose $1 \pm \sqrt{-D} = 2z$. Then $4N(z) = N(1 \pm \sqrt{-D}) = 1 + D \equiv 2 \pmod 4$. A contradiction. ■

5. Show that if $D \equiv 1 \pmod 4$, R is not a PID. (Hint: If R is a PID, $\langle p \rangle$ is a prime ideal whenever p is an irreducible element.)

   Solution. Consider $(1 + \sqrt{-D})(1 - \sqrt{-D}) = 1 + D \in \langle 2 \rangle$. But $1 \pm \sqrt{-D} \notin \langle 2 \rangle$. thus $\langle 2 \rangle$ is not a prime ideal. Since $D \geq 2$ and $D \equiv 1 \pmod 4$, $D \geq 5$. Thus 2 is an irreducible element in R, which is absurd. ■

Quiz 7

(*Due at 1:50 p.m. on Wednesday. Oct. 22, 2008*)

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

Let R be an integral domain. A nonzero element p of R is said to be a *prime element* if $\langle p \rangle = \{rp \mid r \in R\}$ is a prime ideal of R.

1. Show that a prime element is an irreducible element.

2. Let $a \in R$ be a nonzero element and $a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$, where p_i $(i = 1, 2, \ldots, r)$ and q_j $(j = 1, 2, \ldots, s)$ are prime elements. Show that $r = s$ and by reordering q_j's, $p_i = u_i q_i$ with $u_i \in U(R)$ for $i = 1, 2, \ldots, r$, i.e., the uniqueness of prime factorization holds.

3. Show that R is a UFD if and only if every nonzero non-unit element $a \in R$ can be written as a product of prime elements.

Message: Please write your comments and requests.

Solutions to Quiz 7

Let R be an integral domain. A nonzero element p of R is said to be a *prime element* if $\langle p \rangle = \{rp \mid r \in R\}$ is a prime ideal of R.

1. Show that a prime element is an irreducible element.

   Solution. Suppose p is a prime element and $p = xy$, $x, y \in R$. Since $\langle p \rangle$ is a prime ideal, either $x \in \langle p \rangle$ or $y \in \langle p \rangle$. Assume that $x \in \langle p \rangle$ and there exists $z \in R$ such that $x = zp$. Then $p = xy = zyp$. Therefore $zy = 1$ and y is a unit. Similarly if $y \in \langle p \rangle$, then x is a unit. Therefore p is an irreducible element. Note that p is a nonzero element and as $\langle p \rangle$ is a prime ideal and not equal to R, p is not a unit. ■

2. Let $a \in R$ be a nonzero element and $a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$, where p_i ($i = 1, 2, \ldots, r$) and q_j ($j = 1, 2, \ldots, s$) are prime elements. Show that $r = s$ and by reordering q_j's, $p_i = u_i q_i$ with $u_i \in U(R)$ for $i = 1, 2, \ldots, r$, i.e., the uniqueness of prime factorization holds.

   Solution. We proceed by induction on r. If $r = 0$, then a is a unit and $s = 0$. Note that if $s \geq 1$, then $a \in \langle q_1 \rangle \neq R$. Suppose $r \geq 1$. Then $q_1 q_2 \cdots q_s = a = p_1 p_2 \cdots p_r \in \langle p_r \rangle$ and $\langle p_r \rangle$ is a prime ideal. Hence there exists j such that $q_j \in \langle p_r \rangle$. By reordering let $q_s \in \langle p_r \rangle$. Hence there exists $x \in R$ such that $q_s = x p_r$. By 1, q_s is an irreducible element and p_r is not a unit, x is a unit. Hence $p_1 \cdots p_{r-1} p_r = q_1 \cdots q_{s-1} q_s = q_1 \cdots (q_{s-1} x) p_r$ as R is an integral domain. Thus $p_1 \cdots p_{r-1} = q_1 \cdots (q_{s-1} x)$. Since $q_{s-1} x$ is a prime element and by induction hypothesis, we have the assertion. ■

3. Show that R is a UFD if and only if every nonzero non-unit element $a \in R$ can be written as a product of prime elements.

   Solution. Suppose R is a UFD. Since every irreducible element is a prime element in a UFD, every nonzero element $a \in R$ can be written as a product of prime elements.

   Conversely suppose every nonzero element $a \in R$ can be written as a product of prime elements. Then by 1, a can be written as a product of irreducible elements. By 2 the expression is unique modulo ordering and multiplication by unit elements. Therefore R is a UFD. ■

Quiz 8

(*Due at 1:50 p.m. on Wednesday November 5, 2008*)

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

Let $R = \boldsymbol{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \boldsymbol{Z}\}$, and $N(a + b\sqrt{2}) = a^2 - 2b^2$. Show the following.

1. For $\alpha \in R$, $\alpha \in U(R) \Leftrightarrow N(\alpha) = \pm 1$.

2. Show that $U(R) = \{\pm(1 + \sqrt{2})^i \mid i \in \boldsymbol{Z}\}$.

3. Show that R is an Euclidean domain.

4. Express 21 as a product of irreducible elements in R.

Message: Please write your comments and requests.

Solutions to Quiz 8

Let $R = \boldsymbol{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \boldsymbol{Z}\}$, and $N(a + b\sqrt{2}) = a^2 - 2b^2$. Show the following.

1. For $\alpha \in R$, $\alpha \in U(R) \Leftrightarrow N(\alpha) = \pm 1$.

   Solution. First note that $N(\alpha\beta) = N(\alpha)N(\beta)$ for all elements $\alpha, \beta \in R$. Let $\beta \in R$ such that $\alpha\beta = 1$. Then $N(\alpha)N(\beta) = 1$. Since $N(\alpha)$ is an integer, it has to be ± 1. Conversely, if $N(\alpha) = \pm 1$ for $\alpha = a + b\sqrt{2}$. Then $(a + b\sqrt{2})(a - b\sqrt{2}) = N(a + b\sqrt{2})$, and $\alpha^{-1} = N(\alpha)(a - b\sqrt{2})$. ■

2. Show that $U(R) = \{\pm(1 + \sqrt{2})^i \mid i \in \boldsymbol{Z}\}$.

   Solution. Since $N(\pm(1 + \sqrt{2})^i) = N(1 + \sqrt{2})^i = (-1)^i$, $U(R) \supset \{\pm(1 + \sqrt{2})^i \mid i \in \boldsymbol{Z}\}$. Suppose $\alpha \in U(R)$. Since $N(1 + \sqrt{2}) = -1$, we may assume that $N(\alpha) = 1$ by multiplying $1 + \sqrt{2}$ if necessary. By taking $-\alpha$ if necessary, we may assume that $\alpha = u + v\sqrt{2}$ with $u > 0$. Choose α so that u is minimum among α. Then u is odd. Since $(1 \pm \sqrt{2})^2 = 3 \pm 2\sqrt{2}$, we will show that $u = 3$ because $3 \pm 2\sqrt{2}$ are the only solutions with $a = 3$. Suppose $u > 3$. Let $(u + v\sqrt{2})(3 - 2\sqrt{2}) = s + t\sqrt{2}$. Then $s = 3u - 4v$, $t = -2u + 3v$, and $u = 3s + 4t$, $v = 2s + 3t$. Since $s^2 - 2t^2 = 1$, we want to show that $0 < s < u$. First both s and t are positive. Since $u^2 = 1 + 2v^2 > 2v^2$, $u > \sqrt{2}v$. Hence $s = 3u - 4v > 3\sqrt{2}v - 4v = (3\sqrt{2} - 4)v > 0$. Moreover since $u > 3$, $18v^2 = 9(2v^2) = 9(u^2 - 1) = 9u^2 - 9 = 8u^2 + (u^2 - 9) > 8u^2$, $v > \frac{2}{3}u$. Hence $t = -2u + 3v > -2u + 3\frac{2}{3}u = 0$. Therefore $s < u$ as $u = 3s + 4t$. Thus we have the assertion. ■

3. Show that R is an Euclidean domain.

   Solution. Let $\alpha = u + v\sqrt{2}$ and $\beta = s + t\sqrt{2} \neq 0$ be elements of R. Then we can choose $a, b \in \boldsymbol{Z}$ and $c, d \in \boldsymbol{Q}$ such that $\gamma = a + b\sqrt{2} \in R$ and

   $$\frac{\alpha}{\beta} = \frac{u + v\sqrt{2}}{s + t\sqrt{2}} = (a + b\sqrt{2}) + (c + d\sqrt{2}) = \gamma + (c + d\sqrt{2}) \text{ so that } |c| \leq \frac{1}{2},\ |d| \leq \frac{1}{2}.$$

   Since $|N(c + d\sqrt{2})| = |c^2 - 2d^2| \leq \frac{1}{4} + \frac{2}{4} < 1$, $\alpha = \beta\gamma + \rho$, where $\rho = \beta(c + d\sqrt{2}) \in R$ and that $|N(\rho)| < |N(\beta)|$. Hence R is an Euclidean domain with associated function $\delta : R \setminus \{0\} \to \boldsymbol{N}$ $(\alpha \mapsto |N(\alpha)|)$.

   ■

4. Express 21 as a product of irreducible elements in R.

   Solution. $21 = 3 \cdot (3 - \sqrt{2}) \cdot (3 + \sqrt{2})$.

   Since R is an Euclidean domain, it is a UFD. Hence it suffices to show that 3, $3 - \sqrt{2}$ and $3 + \sqrt{2}$ are irreducible elements in R.

   First 3 is irreducible. Suppose not. Then there exist $\alpha, \beta \in R \setminus U(R)$ such that $3 = \alpha\beta$. Hence $N(\alpha) = \pm 3 = a^2 - 2b^2$. Considering modulo 3, we have $a^2 + b^2 \equiv 0 \pmod 3$, which is impossible as squares in $\boldsymbol{Z}_3$ are 0 and 1.

   Finally $3 \pm \sqrt{2}$ are irreducible as $N(3 \pm \sqrt{2}) = 7$. ■