Quiz 1

Due at 10:00 a.m. Wednesday, September 20, 2006

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

1. Let R be a ring. Suppose that a, b are elements of R. Show that $(-a) \cdot (-b) = a \cdot b$. Use only the definition of rings.

2. Let $\boldsymbol{Z}[t]$ be the ring of polynomials in t over the ring of rational integers. If $f, g \in \boldsymbol{Z}[t]$ satisfy $f \cdot g = 1$, i.e., f is a unit and g is its inverse, then $f = \pm 1$.

Message: Any requests?

Solutions to Quiz 1

September 20, 2006

1. Let R be a ring. Suppose that a, b are elements of R. Show that $(-a) \cdot (-b) = a \cdot b$. Use only the definition of rings.

   Solution: Let c be an arbitrary element.

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

   Similarly, $0 \cdot c = 0$. Clearly $-(-c) = c$ as $(-c) + c = 0 = c + (-c)$. Now

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

■

2. Let $\boldsymbol{Z}[t]$ be the ring of polynomials in t over the ring of rational integers. If $f, g \in \boldsymbol{Z}[t]$ satisfy $f \cdot g = 1$, i.e., f is a unit and g is its inverse, then $f = \pm 1$.

   Solution: Let $m = \deg f$ and $n = \deg g$, $f = a_m t^m + \cdots + a_0$ and $g = b_n t^n + \cdots + b_0$. Since $a_m \neq 0$, $b_n \neq 0$ and $a_m, b_n \in \boldsymbol{Z}$, $a_m \cdot b_n \neq 0$. Hence $\deg f \cdot g = m + n$ as $f \cdot g = a_m b_n t^{m+n} + \cdots + a_0 b_0$. On the other hand, $0 = \deg 1 = \deg f \cdot g$ by assumption. Hence $m = n = 0$. In particular, $f = a_0$, $g = b_0$ and $a_0 \cdot b_0 = 1$. Since $a_0, b_0 \in \boldsymbol{Z}$, $a_0 = \pm 1$ and we have the assertion. ■

   Using the notation on page 102, $U(\boldsymbol{Z}[t]) = \{\pm 1\}$. Can you determine $U(\boldsymbol{Z}_4[t])$? Note that $([2]_4 t + [1]_4)([2]_4 t + [1]_4) = [1]_4$.

Quiz 2

Due at 10:00 a.m. Wednesday, September 27, 2006

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

Let R be a ring. Prove the following.

1. Let $x \in R$. Then $Rx = \{r \cdot x \mid r \in R\}$ is a left ideal of R.

2. Let I and J be left ideals of R. Then $I \cap J$ is a left ideal of R.

3. Let I and J be left ideals of R. Then $I + J = \{x + y \mid x \in I,\ y \in J\}$ is a left ideal of R.

4. Let I be a left ideal of R and S a subring of R. Then $I \cap S$ is a left ideal of S.

5. Let I be a left ideal of R. Then $A = \{a \in R \mid ax = 0 \text{ for all } x \in I\}$ is a left ideal of R.

Message: Requests? Questions?

Solutions to Quiz 2

September 27, 2006

Let R be a ring. Prove the following.

In order to show a nonempty subset Y of a ring X is a left ideal, it suffices to show; (i) $a+b \in Y$ whenever $a, b \in Y$, (ii) $-a \in Y$ whenever $a \in Y$ and (iii) $c \cdot a \in Y$ whenever $c \in X$ and $a \in Y$.

By definition a left ideal is an additive subgroup of X satisfying the property (iii) above, and a nonempty subset of a group is a subgroup if it is closed under the binary operation and taking inverse. See (3.3.3) in the textbook. If R has an identity element 1, it is not difficult to show that $(-1)a = -a$. Hence the condition (ii) follows from (iii). But the existence of an identity element is not guaranteed in general.

1. Let $x \in R$. Then $Rx = \{r \cdot x \mid r \in R\}$ is a left ideal of R.

   Solution: Let $a, b \in Rx$. Then by the definition of Rx, there exist $r, s \in R$ such that $a = r \cdot x$ and $b = s \cdot x$. (i) Since $a + b = r \cdot x + s \cdot x = (r + s) \cdot x$ and $r + s \in R$, $a+b \in Rx$. (ii) Since $r \cdot x + (-r) \cdot x = (r + (-r)) \cdot x = 0 \cdot x = 0$, $(-r) \cdot x = -(r \cdot x)$. Hence $-a = -(r \cdot x) = (-r) \cdot x \in Rx$. For the proof of $0 \cdot x = 0$, see Solutions to Quiz 1. (iii) Let $s \in R$. Then $s \cdot a = s \cdot (r \cdot x) = (s \cdot r) \cdot x$ and $s \cdot r \in R$. Hence $s \cdot a \in Rx$. ■

2. Let I and J be left ideals of R. Then $I \cap J$ is a left ideal of R.

   Solution: Let $a, b \in I \cap J$. Then $a, b \in I$ and $a, b \in J$. Since both I and J are left ideals, (i) $a+b \in I$ and $a+b \in J$, hence $a+b \in I \cap J$, (ii) $-a \in I$ and $-a \in J$, hence $-a \in I \cap J$, (iii) $r \cdot a \in I$ and $r \cdot a \in J$, hence $r \cdot a \in I \cap J$ whenever $r \in R$. Therefore $I \cap J$ is a left ideal of R. ■

3. Let I and J be left ideals of R. Then $I + J = \{x + y \mid x \in I,\ y \in J\}$ is a left ideal of R.

   Solution: Let $a, b \in I + J$. Then by the definition of $I + J$, there exist $x, x' \in I$ and $y, y' \in J$ such that $a = x + y$ and $b = x' + y'$. Now we use the fact that both I and J are left ideals. (i) Since $a+b = (x+y)+(x'+y') = (x+x')+(y+y') \in I+J$ and $x+x' \in I$, $y + y' \in J$, $a + b \in I + J$. (ii) $-a = -(x + y) = (-x) + (-y) \in I + J$ as $-x \in I$ and $-y \in J$. (iii) Let $r \in R$. Then $r \cdot a = r \cdot (x + y) = r \cdot x + r \cdot y$ and $r \cdot x \in I$ and $r \cdot y \in J$. Hence $r \cdot a \in I + J$. ■

4. Let I be a left ideal of R and S a subring of R. Then $I \cap S$ is a left ideal of S.

   Solution: (i) and (ii) follow from the proof of 2. Let $s \in S$ and $x \in I \cap S$. Since I is a left ideal of R and $s \in S \subset R$, $s \cdot x \in I$. Since S is a subring and $s, x \in S$, $s \cdot x \in S$. Hence $s \cdot x \in I \cap S$. This proves (iii) and $I \cap S$ is a left ideal of S. ■

5. Let I be a left ideal of R. Then $A = \{a \in R \mid ax = 0 \text{ for all } x \in I\}$ is a left ideal of R.

   Solution: Let $a, b \in A$. Then $a \cdot x = 0 = b \cdot x$ whenever $x \in I$. Let x be an arbitrary element of I. (i) Since $(a + b) \cdot x = a \cdot x + b \cdot x = 0 + 0 = 0$, $a + b \in A$. (ii) As in the proof of 1, $(-a) \cdot x = -(ax)$. Hence $(-a) \cdot x = 0$. Therefore $-a \in A$. (iii) Let $r \in R$. Then $(r \cdot a) \cdot x = r \cdot (a \cdot x) = r \cdot 0 = 0$. Hence $r \cdot a \in A$ and A is a left ideal of R. ■

Quiz 3

Due at 10:00 a.m. Wednesday, October 4, 2006

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

Let $R = \boldsymbol{Z}_{18}$.

1. Find all zero divisors of R.

2. Find $U(R)$, i.e, the set of all units in R.

3. Find a prime ideal I of R.

4. Let I be the prime ideal chosen in the previous problem. Determine whether R/I is a field.

5. Find all proper deals of R which are not prime ideals. Note that an ideal J of R is proper if $J \neq R$.

Message: Requests? Questions?

Solutions to Quiz 3

October 4, 2006

Let $R = \boldsymbol{Z}_{18} = \{[0],[1],[2],[3],[4],[5],[6],[7],[8],[9],[10],[11],[12],[13],[14],[15],[16],[17]\}$.

1. Find all zero divisors of R.

   Solution: Let $\mathrm{ZD}(R)$ denote the set of all zero devisors of R. Since R is a commutative ring,
   $$\mathrm{ZD}(R) = \{a \in R \mid (a \neq 0) \wedge (\exists b \in R)[(b \neq 0) \wedge (a \cdot b = 0)]\}.$$
   Hence
   $$\mathrm{ZD}(R) = \{[2],[3],[4],[6],[8],[9],[10],[12],[14],[15],[16]\}.$$

2. Find $U(R)$, i.e, the set of all units in R.

   Solution: Since R is a commutative ring,
   $$U(R) = \{a \in R \mid (\exists b \in R)[a \cdot b = 1]\} = \{a \in R \mid a \cdot b = 1 \text{ for some } b \in R\}.$$
   Hence
   $$U(R) = \{[1],[5],[7],[11],[13],[17]\}.$$

3. Find a prime ideal I of R.

   Solution: Let $I = \{[0],[2],[4],[6],[8],[10],[12],[14],[16]\}$. Since $I = R \cdot [2]$, I is of form Rx with $x \in R$, and I is an ideal. See Quiz 2, Problem 1. Since every ideal is an additive subgroup of R, if J with $I \subset J \subset R$ is an ideal of R, $|J|$ is a divisor of $|R| = 18$. Since $|I| = 9$ and $I \subset J$, $I = J$ or $J = R$. Hence I is a maximal ideal. Therefore I is a prime ideal. (6.3.7). ■

   $I' = \{[0],[3],[6],[9],[12],[15]\}$ is also a prime ideal. I' is a maximal ideal as well. It is not so difficult to check that there are no other prime ideals. So in this particular case, I is a prime ideal if and only if I is a maximal ideal.

4. Let I be the prime ideal chosen in the previous problem. Determine whether R/I is a field.

   Solution: As we have seen above, I is a maximal ideal. Hence by (6.3.7) in the textbook, R/I is a field. ■

   Note that $R/I = \{I, [1]+I\}$ and it is isomorphic to $\boldsymbol{Z}_2$, a field with two elements. $R/I' = \{I', [1]+I', [2]+I'\}$ is isomorphic to $\boldsymbol{Z}_3$. .

5. Find all proper deals of R which are not prime ideals. Note that an ideal J of R is proper if $J \neq R$.

   Solution: As an additive group R is a cyclic group and all of its subgroup is cyclic. Hence all ideals of R are of form $R \cdot x$. Hence $R \cdot [0] = \{[0]\}$, $R \cdot [6] = \{[0],[6],[12]\}$, $R \cdot [9] = \{[0],[9]\}$. ■

   Note that if x is a unit, $Rx = R$. So we must choose non-units. Please refer to (4.1.7).

Take-Home Midterm *Due: 10:00 a.m. October 11, 2006*

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

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

   (a) For a, $b \in R$, $(-a) \cdot b = (-1) \cdot a \cdot b$.

   (b) There exist nonzero elements a, $b \in R$, $a \cdot b = 0$.

   (c) For elements a, $b \in R$, $a \cdot b - b \cdot a = 0$.

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

2. Show that the polynomial ring $R[t, u] = (R[t])[u]$ with two indeterminates t and u over an integral domain R is an integral domain.

3. Let R be an integral domain. For $a, b \in R$, suppose $R \cdot a = R \cdot b$. Then there exists a unit $u \in U(R)$ such that $b = ua$.

4. Let R and R' be commutative rings with identity. Suppose $\alpha : R \to R'$ is a ring homomorphism, I is an ideal of R and J is an ideal of R'.

   (a) Show that $\alpha^{-1}(J) = \{x \in R \mid \alpha(x) \in J\}$ is an ideal of R.

   (b) Show that $\alpha^{-1}(\alpha(I)) = I + \mathrm{Ker}(\alpha)$.

5. Let $\boldsymbol{Z}[t]$ be a polynomial ring over $\boldsymbol{Z}$ and $R = \{f(\sqrt{-1}) \mid f(t) \in \boldsymbol{Z}[t]\}$.

(a) Let $\alpha : \boldsymbol{Z}[t] \to \boldsymbol{C}$ $(f(t) \mapsto f(\sqrt{-1}))$. Then α is a ring homomorphism.

(b) Show that $R = \{a + b\sqrt{-1} \mid a,\ b \in \boldsymbol{Z}\}$, and R is an integral domain.

(c) $\boldsymbol{Z}[t](t^2 + 1)$ is a prime ideal of $\boldsymbol{Z}[t]$.

(d) Show that $\boldsymbol{Z}[t](t^2 + 1)$ is not a maximal ideal of $\boldsymbol{Z}[t]$.

Message: Requests? Questions?

Solutions to Midterm

October 11, 2006

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

   (a) For a, $b \in R$, $(-a) \cdot b = (-1) \cdot a \cdot b$.
   Solution: It suffices to show that $-a = (-1) \cdot a$. Recall that $0 \cdot a = 0$. (See Quiz 1.)

   $$-a = (-a) + (1 + (-1)) \cdot a = (-a) + 1 \cdot a + (-1) \cdot a = (-a) + a + (-1) \cdot a = (-1) \cdot a.$$

   Hence $-a = (-1) \cdot a$ and $(-a) \cdot b = (-1) \cdot a \cdot b$ for all $a, b \in R$. ■

   (b) For nonzero elements a, $b \in R$, $a \cdot b = 0$. (I meant the following: There exist nonzero elements a, $b \in R$, $a \cdot b = 0$.)
   Solution: Let $R = \boldsymbol{Z}_4 = \{[0]_4, [1]_4, [2]_4, [3]_4\}$. While $[2]_4 \neq [0]_4 = 0_R$, $[2]_4 \cdot [2]_4 = [0]_4 = 0_R$. ■

   (c) For elements a, $b \in R$, $a \cdot b - b \cdot a = 0$.
   Solution: Let $R = \mathrm{Mat}_2(\boldsymbol{R})$ be the 2×2 matrix ring over the reals. Let

   $$a = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \text{ and } b = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

   Then

   $$\begin{aligned} a \cdot b - b \cdot a &= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}. \end{aligned}$$

   (d) Let f and g be polynomials in $R[t]$. Then $\deg(f) + \deg(g) \geq \deg(fg)$.
   Solution: Let $f = a_m t^m + a_{m-1} t^{m-1} + \cdots + a_0$ and $g = b_n t^n + b_{n-1} t^{n-1} + \cdots + b_0$. Suppose $a_m \neq 0 \neq b_n$. Then $\deg f = m$ and $\deg g = n$. Since

   $$f \cdot g = a_m b_n t^{m+n} + (a_m b_{n-1} + a_{m-1} b_n) t^{m+n-1} + \cdots + a_0 b_0,$$

   $\deg(f \cdot g) \leq m + n = \deg f + \deg g$. Note that if R is a domain, then equality holds in the equation as $a_m b_n \neq 0$. ■

2. Show that the polynomial ring $R[t,u] = (R[t])[u]$ with two indeterminates t and u over an integral domain R is an integral domain.

   Solution: As we have seen in 1 (d), we have $\deg(f)+\deg(g) = \deg(fg)$ if R is a domain. Hence if $f \cdot g = 0$ in $R[t]$, $-\infty = \deg 0 = \deg f \cdot g = \deg f + \deg g$ implies that at least one of $\deg f$ or $\deg g$ is $-\infty$. Hence either $f = 0$ or $g = 0$. Thus $R[t]$ is a domain. Therefore in general, if R is a domain, $R[t]$ is a domain. Since $R[t,u]$ is a polynomial ring over a domain $R[t]$, $R[t,u]$ is also a domain as well. ■

3. Let R be an integral domain. For $a, b \in R$, suppose $R \cdot a = R \cdot b$. Then there exists a unit $u \in U(R)$ such that $b = ua$.

   Solution: Suppose $R \cdot a = R \cdot b$. By definition of a ring with identity, $1 \neq 0$ and $R \neq \{0\}$. See page 97. So if $a = 0$, then $b = 1 \cdot b \in R \cdot b = R \cdot a = \{0\}$ implies that $b = 0$. In this case $a = 0 = 1 \cdot 0 = 1 \cdot b$, and the assertion holds. Hence we may assume that $a \neq 0$. Since $a \in R \cdot a = R \cdot b$, there exists $r \in R$ such that $a = r \cdot b$. Similarly, since $b \in R \cdot b = R \cdot a$, there exists $s \in R$ such that $b = u \cdot a$.

   $$(r \cdot u - 1) \cdot a = r \cdot u \cdot a - a = r \cdot b - a = a - a = 0.$$

   Since $a \neq 0$ and R is an integral domain, $r \cdot u - 1 = 0$ and $r \cdot u = 1$. Thus u is a unit. Note that an integral domain is commutative. Hence $b = u \cdot a$ and u is a unit, as desired. ■

4. Let R and R' be commutative rings with identity. Suppose $\alpha : R \to R'$ is a ring homomorphism, I is an ideal of R and J is an ideal of R'.

   (a) Show that $\alpha^{-1}(J) = \{x \in R \mid \alpha(x) \in J\}$ is an ideal of R.

   Solution: Fist note that $\alpha(0) = 0$ and $\alpha(-x) = -\alpha(x)$ as α is a homomorphism. In particular, $0 \in \alpha^{-1}(J)$ and $\alpha^{-1}(J) \neq \emptyset$. Let $a, b \in \alpha^{-1}(J)$ and $r \in R$. Then

   $$\alpha(a+b) = \alpha(a) + \alpha(b) \in J,\ \alpha(-a) = -\alpha(a) \in J, \text{ and } \alpha(r \cdot a) = \alpha(r) \cdot \alpha(a) \in J$$

   as J is an ideal in R'. Hence $a + b \in \alpha^{-1}(J)$, $-a \in \alpha^{-1}(J)$ and $r \cdot a \in \alpha^{-1}(J)$. Therefore $\alpha^{-1}(J)$ is an ideal in R. ■

   (b) Show that $\alpha^{-1}(\alpha(I)) = I + \mathrm{Ker}(\alpha)$.

   Solution: In the following we do not need the fact that I is an ideal in R. Assume that I is a subset of R. Let $x \in I + \mathrm{Ker}(\alpha)$. Then there exists $a \in I$ and $b \in \mathrm{Ker}(\alpha)$ such that $x = a+b$. Since $\alpha(x) = \alpha(a+b) = \alpha(a)+\alpha(b) = \alpha(a) \in \alpha(I)$, $x \in \alpha^{-1}(\alpha(I))$. Hence $I + \mathrm{Ker}(\alpha) \subset \alpha^{-1}(\alpha(I))$.

   Let $x \in \alpha^{-1}(\alpha(I))$. Then by definition, $\alpha(x) \in \alpha(I)$. Hence there exists $a \in I$ such that $\alpha(x) = \alpha(a)$. Now $\alpha(x - a) = \alpha(x) - \alpha(a) = 0$. Hence $x - a \in \mathrm{Ker}(\alpha)$. Let $b \in \mathrm{Ker}(\alpha)$ such that $x - a = b$. Then $x = a + b \in I + \mathrm{Ker}(\alpha)$. Thus $\alpha^{-1}(\alpha(I)) \subset I + \mathrm{Ker}(\alpha)$. Therefore, $\alpha^{-1}(\alpha(I)) = I + \mathrm{Ker}(\alpha)$. ■

5. Let $\boldsymbol{Z}[t]$ be a polynomial ring over $\boldsymbol{Z}$ and $R = \{f(\sqrt{-1}) \mid f(t) \in \boldsymbol{Z}[t]\}$.

(a) Let $\alpha : \boldsymbol{Z}[t] \to \boldsymbol{C}$ $(f(t) \mapsto f(\sqrt{-1}))$. Then α is a ring homomorphism.
Solution: This is almost clear. See Exercise 6.2.7. Let $f(t), g(t) \in \boldsymbol{Z}[t]$. Then

$$\begin{aligned} \alpha(f(t)+g(t)) &= f(\sqrt{-1}) + g(\sqrt{-1}) = \alpha(f(t)) + \alpha(g(t)), \text{ and} \\ \alpha(f(t)\cdot g(t)) &= f(\sqrt{-1}) \cdot g(\sqrt{-1}) = \alpha(f(t)) \cdot \alpha(g(t)). \end{aligned}$$

Hence α is a ring homomorphism. $\blacksquare$

(b) Show that $R = \{a + b\sqrt{-1} \mid a,\ b \in \boldsymbol{Z}\}$, and R is an integral domain.
Solution: By definition, $R = \mathrm{Im}(\alpha) \subset \boldsymbol{C}$. Since α is a ring homomorphism, R is a subring of a field $\boldsymbol{C}$. Since $\boldsymbol{C}$ does not have a zero-divisor, R is an integral domain. Since for any nonnegative integer n, $\alpha(t^{2n}) = \sqrt{-1}^{2n} = (-1)^n$, and $\alpha(t^{2n+1}) = \sqrt{-1}^{2n+1} = (-1)^n\sqrt{-1}$, $R = \{f(\sqrt{-1}) \mid f(t) \in \boldsymbol{Z}[t]\} \subset \{a + b\sqrt{-1} \mid a,\ b \in \boldsymbol{Z}\}$. Since $\alpha(a+bt) = a+b\sqrt{-1}$, the other inclusion, $R = \{f(\sqrt{-1}) \mid f(t) \in \boldsymbol{Z}[t]\} \supset \{a+b\sqrt{-1} \mid a,\ b \in \boldsymbol{Z}\}$ is clear. Hence we have $R = \{a + b\sqrt{-1} \mid a,\ b \in \boldsymbol{Z}\}$. $\blacksquare$

(c) $\boldsymbol{Z}[t](t^2+1)$ is a prime ideal of $\boldsymbol{Z}[t]$.
Solution: By First Isomorphism Theorem (6.2.4), $R = \mathrm{Im}(\alpha) \simeq \boldsymbol{Z}[t]/\mathrm{Ker}(\alpha)$. Hence by (6.3.7), $\mathrm{Ker}(\alpha)$ is a prime ideal as $1 \notin \mathrm{Ker}(\alpha)$ and $\mathrm{Ker}(\alpha) \neq R$. Let $I = \boldsymbol{Z}[t](t^2+1)$. Since $t^2+1 \in \mathrm{Ker}(\alpha)$, it is clear that $I \subset \mathrm{Ker}(\alpha)$. Let $f(t) \in \mathrm{Ker}(\alpha)$. Then there exists a polynomial $g(t)$ such that $f(t) = g(t)(t^2+1) + a \cdot t + b$. Since $f(t) \in \mathrm{Ker}(\alpha)$,

$$0 = \alpha(f(t)) = f(\sqrt{-1}) = g(\sqrt{-1})(\sqrt{-1}^2 + 1) + a \cdot \sqrt{-1} + b = a\sqrt{-1} + b.$$

Since a and b are integers, $a = b = 0$ and $f(t) = g(t)(t^2+1)$. Therefore, $f(t) \in \boldsymbol{Z}[t](t^2+1)$ and $\mathrm{Ker}(\alpha) = \boldsymbol{Z}[t](t^2+1)$. Therefore, $\boldsymbol{Z}[t](t^2+1)$ is a prime ideal. $\blacksquare$

(d) Show that $\boldsymbol{Z}[t](t^2+1)$ is not a maximal ideal of $\boldsymbol{Z}[t]$.
Solution: Suppose $\boldsymbol{Z}[t](t^2+1)$ is a maximal ideal, then $R \simeq \boldsymbol{Z}[t]/\boldsymbol{Z}[t](t^2+1)$ is a field. But $2^{-1} \notin R$ and R is not a field. Hence $\boldsymbol{Z}[t](t^2+1)$ is not a maximal ideal. $\blacksquare$
Note that $\boldsymbol{Z}[t](t^2+1) \subset \boldsymbol{Z}[t](t^2+1) + \boldsymbol{Z}[t]\cdot 2 \subset \boldsymbol{Z}[t]$.

Quiz 4

Due: 10:00 a.m. October 18, 2006

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

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

   (a) $a \in U(R)$ if and only if $R \cdot a = R$.

   (b) Let a be a nonzero element of R and $a \notin U(R)$. Then a is an irreducible element in R if and only if $R \cdot a \subset R \cdot b \subset R$ implies $R \cdot a = R \cdot b$ or $R \cdot b = R$.

2. Let $R = \{a + b\sqrt{-3} \mid a, b \in \boldsymbol{Z}\}$. Let $N : R \to \boldsymbol{Z}$ ($\alpha = a + b\sqrt{-3} \mapsto N(\alpha) = a^2 + 3b^2$).

   (a) Show that R is an integral domain.

   (b) Show that for $\alpha, \beta \in R$, $N(\alpha \cdot \beta) = N(\alpha)N(\beta)$.

   (c) Show that $\alpha \in U(R) \Leftrightarrow N(\alpha) = 1 \Leftrightarrow \alpha = \pm 1$.

Message: : Requests? Questions?

Solutions to Quiz 4

October 18, 2006

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

   (a) $a \in U(R)$ if and only if $R \cdot a = R$.

   Solution: Suppose $a \in U(R)$. Then for every $x \in R$, $x = x(a^{-1}a) = (xa^{-1})a \in R{\cdot}a$. Hence $R \subset R{\cdot}a$. Therefore $R{\cdot}a = R$. Conversely assume $R{\cdot}a = R$. Since $1 \in R = R{\cdot}a$, there exists $b \in R$ such that $b \cdot a = 1$. Since R is commutative, $a \in U(R)$. ■

   N.B. This directly follows from Problem 3 in Take Home Midterm by setting $b = 1$.

   (b) Let a be a nonzero element of R and $a \notin U(R)$. Then a is an irreducible element in R if and only if $R \cdot a \subset R \cdot b \subset R$ implies $R \cdot a = R \cdot b$ or $R \cdot b = R$.

   Solution: Suppose a is irreducible and $R \cdot a \subset R \cdot b \subset R$. Since $a \in R \cdot a \subset R \cdot b$, there exists $c \in R$ such that $a = c \cdot b$. Since a is irreducible, $c \in U(R)$ or $b \in U(R)$. If $c \in U(R)$ by Problem 3 in Take Home Midterm, $R \cdot a = R \cdot b$. If $b \in U(R)$, then $R \cdot b = R$ by Problem 1. Hence $R \cdot a \subset R \cdot b \subset R$ implies $R \cdot a = R \cdot b$ or $R \cdot b = R$ in this case.

   Conversely suppose $a = c \cdot b$ with $c, b \in R$. Since $a \in R \cdot b$, $R \cdot a \subset R \cdot b \subset R$. Now by our assumption, $R \cdot a = R \cdot b$ or $R \cdot b = R$. If $R \cdot b = R$, then by Problem 1, $b \in U(R)$. On the other hand if $R \cdot a = R \cdot b$, then by Problem 3 in Take Home Midterm, there exists $u \in U(R)$ such that $a = u \cdot b$. Since $a = b \cdot c$, $0 = a - a = b \cdot (u - c)$. If $b = 0$, then $R \cdot a = R \cdot b = \{0\}$ which is absurd as $a \neq 0$. Hence $u = c$ as R is an integral domain. Therefore, $a = c \cdot b$ with $c, b \in R$ implies $b \in U(R)$ or $c \in U(R)$ and a is irreducible. ■

2. Let $R = \{a + b\sqrt{-3} \mid a, b \in \boldsymbol{Z}\}$. Let $N : R \to \boldsymbol{Z}$ ($\alpha = a + b\sqrt{-3} \mapsto N(\alpha) = a^2 + 3b^2$).

   (a) Show that R is an integral domain.

   Solution: As in Problem 5 (a), (b) in Take Home Midterm, $\alpha : \boldsymbol{Z}[t] \to \boldsymbol{C}$ ($f(t) \mapsto f(\sqrt{-3})$) is a ring homomorphism. Hence its image R is a subring of $\boldsymbol{C}$. Since $\boldsymbol{C}$ does not have a zero divisor, R is an integral domain. ■

   (b) Show that for $\alpha, \beta \in R$, $N(\alpha \cdot \beta) = N(\alpha)N(\beta)$.

   Solution: Let $\alpha = a + b\sqrt{-3}$ and $\beta = c + d\sqrt{-3}$. Then

$$\begin{aligned} N(\alpha \cdot \beta) &= N((ac - 3bd) + (ad + bc)\sqrt{-3})) = (ac - 3bd)^2 + 3(ad + bc)^2 \\ &= a^2c^2 - 6abcd + 9b^2d^2 + 3a^2d^2 + 6abcd + 3b^2c^2 \\ &= (a^2 + 3b^2)(c^2 + 3d^2) = N(\alpha)N(\beta). \quad ■ \end{aligned}$$

   The fact also follows from the property of complex conjugate as $\overline{\alpha \cdot \beta} = \overline{\alpha}\overline{\beta}$ and $N(\alpha) = \alpha \cdot \overline{\alpha}$.

   (c) Show that $\alpha \in U(R) \Leftrightarrow N(\alpha) = 1 \Leftrightarrow \alpha = \pm 1$.

   Solution: Suppose $\alpha \in U(R)$. Then $\alpha\beta = 1$ implies $N(\alpha)N(\beta) = N(1) = 1$. Since $N(\alpha)$ and $N(\beta)$ are both nonnegative integers, $N(\alpha) = 1$. Conversely if $N(\alpha) = 1$, then $\alpha \cdot \overline{\alpha} = N(\alpha) = 1$. Hence, $\alpha \in U(R)$. Since $N(\alpha) = a^2 + 3b^2$. it is clear that $N(\alpha) = 1$ if and only if $\alpha = \pm 1$. ■

Quiz 5

Due: 10:00 a.m. October 25, 2006

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

1. Let R be an integral domain, and p a nonzero element in R. Show the following.
   (a) If $I = \langle p \rangle$ is a prime ideal, then p is an irreducible element.

   (b) If R is a principal ideal domain and p is an irreducible element, then $I = \langle p \rangle$ is a maximal ideal.

2. Let $R = \boldsymbol{Z}[t]$, the polynomial ring over $\boldsymbol{Z}$. Show the following.
   (a) $U(R) = \{\pm 1\}$ and t is an irreducible element in R.

   (b) Let $\alpha : R = \boldsymbol{Z}[t] \to \boldsymbol{Z}$ $(f(t) \mapsto f(0))$. Then α is a surjective homomorphism and $\mathrm{Ker}(\alpha) = \boldsymbol{Z}[t] \cdot t$.

   (c) R is not a principal ideal domain.

Message: Requests? Questions?

Solutions to Quiz 5

October 25, 2006

1. Let R be an integral domain, and p a nonzero element in R. Show the following.

   (a) If $I = \langle p \rangle$ is a prime ideal, then p is an irreducible element.

   Solution: Since I is a prime ideal, $I \neq R$. Hence p is not a unit. (Quiz 4 1(a)) Suppose $p = a \cdot b$. Since $a \cdot b \in \langle p \rangle = I$ and I is a prime ideal, $a \in I$ or $b \in I$. Since $I = \langle p \rangle$, $p \mid a$ or $p \mid b$. If $p \mid a$, then there exists $u \in R$ such that $a = p \cdot u$ and that $p = p \cdot u \cdot b$. Hence $p \cdot (1 - u \cdot b) = 0$. Since $p \neq 0$ and R is an integral domain, we have $u \cdot b = 1$. Thus $b \in U(R)$. If $p \mid b$, we similarly obtain $a \in U(R)$. Therefore, p is irreducible. ■

   (b) If R is a principal ideal domain and p is an irreducible element, then $I = \langle p \rangle$ is a maximal ideal.

   Solution: Suppose J is an ideal such that $I \subset J \subset R$. Since R is a PID, there exists $a \in R$ such that $J = \langle a \rangle$. Since $p \in I \subset J = \langle a \rangle$, there exists $b \in R$ such that $p = a \cdot b$. Hence either $a \in U(R)$ or $b \in U(R)$ and $\langle a \rangle = \langle p \rangle$. Therefore $J = \langle a \rangle = I$ or $J = R$, and I is a maximal ideal. ■

2. Let $R = \boldsymbol{Z}[t]$, the polynomial ring over $\boldsymbol{Z}$. Show the following.

   (a) $U(R) = \{\pm 1\}$ and t is an irreducible element in R.

   Solution: Suppose $f \cdot g = 1$. Then $0 = \deg(f \cdot g) = \deg(f) + \deg(g)$. (Note that this formula holds as $\boldsymbol{Z}$ is an integral domain.) Hence both f and g are in $\boldsymbol{Z}$. Hence $\deg(f) = \deg(g) = 0$ and $f, g \in \{\pm 1\}$. Thus $U(R) = \{\pm 1\}$. t is nonzero and $t \notin U(R)$. If $t = f \cdot g$ in R, then $1 = \deg(t) = \deg(f \cdot g) = \deg(f) + \deg(g)$. Hence we may assume that $f \in \boldsymbol{Z}$ and $g = a \cdot t + b$ where $a, b \in \boldsymbol{Z}$ and $a \neq 0$. Then $f \cdot a = 1$ and $f \in U(R)$. Therefore, t is irreducible. ■

   (b) Let $\alpha : R = \boldsymbol{Z}[t] \to \boldsymbol{Z}$ $(f(t) \mapsto f(0))$. Then α is a surjective homomorphism and $\mathrm{Ker}(\alpha) = \boldsymbol{Z}[t] \cdot t$.

   Solution: It is clear that α is a ring homomorphism. It is also clear that $\mathrm{Ker}(\alpha) = \boldsymbol{Z}[t] \cdot t$. (Let $\mathrm{Ker}(\alpha) \ni f(t) = a_0 + a_1 t + \cdots + a_n t^n$ and observe that $a_0 = 0$.) ■

   (c) R is not a principal ideal domain.

   Solution: Since $R/\mathrm{Ker}(\alpha) \simeq \boldsymbol{Z}$ and $\boldsymbol{Z}$ is not a field, $\mathrm{Ker}(\alpha)$ is not a maximal ideal. If R is a principal ideal, the ideal $I = \langle t \rangle$ is an ideal generated by an irreducible element. Therefore by 1(b), I is maximal. This is a contradiction. Thus, R is not a PID. ■

Quiz 6

Due: 10:00 a.m. October 30, 2006

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

Let R be an integral domain and P a prime ideal of R. Set $S = R \setminus P = \{x \in R \mid x \notin P\}$. We define a relation on $R \times S$ by the following: $(a, s) \sim (b, t) \Leftrightarrow a \cdot t - b \cdot s = 0$. Let $a/s = \{(b, t) \in R \times S \mid (a, s) \sim (b, t)\}$. Show the following.

1. $0 \notin S$, $1 \in S$ and $s, t \in S$ implies $s \cdot t \in S$.

2. The relation $\sim$ on $R \times S$ is an equivalence relation.

3. Let $S^{-1}R = \{a/s \mid a \in R \wedge s \in S\}$, the set of all equivalence classes. Define

$$a/s + b/t = (a \cdot t + b \cdot s)/(s \cdot t) \text{ and } (a/s) \cdot (b/t) = (a \cdot b)/(s \cdot t).$$

   Then these binary operations are well-defined and $S^{-1}R$ is an integral domain.

4. Let $P^* = \{p/s \mid p \in P, s \in S\} \subset S^{-1}R$. Then P^* is the only maximal ideal in $S^{-1}R$.

Message: Requests? Questions?

Solutions to Quiz 6

October 30, 2006

Let R be an integral domain and P a prime ideal of R. Set $S = R \setminus P = \{x \in R \mid x \notin P\}$. We define a relation on $R \times S$ by the following: $(a, s) \sim (b, t) \Leftrightarrow a \cdot t - b \cdot s = 0$. Let $a/s = \{(b, t) \in R \times S \mid (a, s) \sim (b, t)\}$. Show the following.

1. $0 \notin S$, $1 \in S$ and $s, t \in S$ implies $s \cdot t \in S$.

   Solution: Since $0 \in P$, $0 \notin S$. Since $P \neq R$, $1 \notin P$ and $1 \in S$. Suppose $s \cdot t \notin S$. Then $s \cdot t \in P$. Since P is a prime ideal, either $s \in P$ or $t \in P$. Hence $s \notin S$ or $t \notin S$. This shows the contraposition of the fact that $s, t \in S$ implies $s \cdot t \in S$. Thus we have all the assertions. ■

2. The relation $\sim$ on $R \times S$ is an equivalence relation.

   Solution: (i) Since $a \cdot s - a \cdot s = 0$, $(a, s) \sim (a, s)$ for all $a \in R$, $s \in S$.

   (ii) Suppose $(a, s) \sim (b, t)$. Then $a \cdot t - b \cdot s = 0$. Hence $b \cdot s - a \cdot t = 0$, which implies $(b, t) \sim (a, s)$.

   (iii) Suppose $(a, s) \sim (b, t)$ and $(b, t) \sim (c, u)$. Then we have $a \cdot t - b \cdot s = b \cdot u - c \cdot t = 0$. Since

$$\begin{aligned} (a \cdot u - c \cdot s) \cdot t &= a \cdot t \cdot u - c \cdot t \cdot s = a \cdot t \cdot u - b \cdot s \cdot u + b \cdot u \cdot s - c \cdot t \cdot s \\ &= (a \cdot t - b \cdot s) \cdot u + (b \cdot u - c \cdot t) \cdot s = 0, \end{aligned}$$

   $a \cdot u - c \cdot s = 0$ as R is an integral domain and $t \in S$, $0 \notin S$. we have $(a, s) \sim (c, u)$.

   Therefore the relation $\sim$ is an equivalence relation. ■

3. Let $S^{-1}R = \{a/s \mid a \in R \wedge s \in S\}$, the set of all equivalence classes. Define

$$a/s + b/t = (a \cdot t + b \cdot s)/(s \cdot t) \text{ and } (a/s) \cdot (b/t) = (a \cdot b)/(s \cdot t).$$

   Then these binary operations are well-defined and $S^{-1}R$ is an integral domain.

   Solution: Suppose $(a, s) \sim (a', s')$ and $(b, t) \sim (b', t')$. We show that

$$(a \cdot t + b \cdot s, s \cdot t) \sim (a' \cdot t' + b' \cdot s', s' \cdot t'), \text{ and } (a \cdot b, s \cdot t) \sim (a' \cdot b', s' \cdot t').$$

$$\begin{aligned} &(a \cdot t + b \cdot s)(s' \cdot t') - (a' \cdot t' + b' \cdot s')(s \cdot t) \\ &= (a \cdot s' \cdot t \cdot t' - a' \cdot s \cdot t \cdot t') + (b \cdot t' \cdot s \cdot s' - b' \cdot t \cdot s \cdot s') \\ &= (a \cdot s' - a' \cdot s) \cdot t \cdot t' + (b \cdot t' - b' \cdot t) \cdot s \cdot s' = 0, \end{aligned}$$

$$\begin{aligned} a \cdot b \cdot s' \cdot t' - a' \cdot b' \cdot s \cdot t &= a \cdot b \cdot s' \cdot t' - a' \cdot b \cdot s \cdot t' + a' \cdot b \cdot s \cdot t' - a' \cdot b' \cdot s \cdot t \\ &= (a \cdot s' - a' \cdot s) \cdot b \cdot t' + a' \cdot s \cdot (b \cdot t' - b' \cdot t) = 0. \end{aligned}$$

   Hence binary operations are well-defined. Now other properties of commutative rings with identity are easy to prove. Note that for all $s \in S$, $0/s = 0/1 = 0_{S^{-1}R}$ and $s/s = 1/1 = 1_{S^{-1}R}$. Moreover if $(a/s) \cdot (b/t) = 0/1$. Then $0 = a \cdot b \cdot 1 - s \cdot t \cdot 0 = a \cdot b$. Since R is an integral domain, we have $a = 0$ or $b = 0$, and $S^{-1}R$ is an integral domain. ■

4. Let $P^* = \{p/s \mid p \in P, s \in S\} \subset S^{-1}R$. Then P^* is the only maximal ideal in $S^{-1}R$.

   Solution: It is clear that P^* is an ideal of $S^{-1}P$. If $s, t \in S$, then $s/t \in U(S^{-1}R)$ and hence $S^{-1}R \setminus P^* = U(S^{-1}R)$. Therefore P^* is the unique maximal ideal of $S^{-1}R$. ■

Quiz 7

Due: 10:00 a.m. November 6, 2006

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

Let $R = \boldsymbol{Z}[\sqrt{10}] = \{a + b\sqrt{10} \mid a, b \in \boldsymbol{Z}\}$, and $N(a + b\sqrt{10}) = a^2 - 10b^2$. Show the following.

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

2. There are infinitely many units in R. (Hint: Firstly find one, say α. Show that α^n are all distinct.)

3. For $\alpha \in R$, $N(\alpha) \neq \pm 2, \pm 3$. (Hint: Use the fact that in $\boldsymbol{Z}_5$, $\{a^2 \mid a \in \boldsymbol{Z}_5\} = \{[0], [1], [4]\}$.)

4. 3 is an irreducible element in R.

5. R is not a UFD. (Hint: Check whether $I = \langle 3 \rangle$ is a prime ideal or not.)

Message: Requests? Questions?

Solutions to Quiz 7

November 6, 2006

Let $R = \boldsymbol{Z}[\sqrt{10}] = \{a + b\sqrt{10} \mid a, b \in \boldsymbol{Z}\}$, and $N(a + b\sqrt{10}) = a^2 - 10b^2$. 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 $\alpha = a + b\sqrt{10}$. Then $(a + b\sqrt{10})(a - b\sqrt{10}) = N(a + b\sqrt{10})$, and $\alpha^{-1} = N(\alpha)(a - b\sqrt{10})$. ■

2. There are infinitely many units in R. (Hint: Firstly find one, say α. Show that α^n are all distinct.)

   Solution: By 1, $\alpha = 3 - \sqrt{10} \in U(R)$. Since $|\alpha| \neq 1$, $\alpha^i = \alpha^j$ if and only if $i = j$. Since $\alpha^i \in U(R)$, there are infinitely many units in R. ■

3. For $\alpha \in R$, $N(\alpha) \neq \pm 2, \pm 3$. (Hint: Use the fact that in $\boldsymbol{Z}_5$, $\{a^2 \mid a \in \boldsymbol{Z}_5\} = \{[0], [1], [4]\}$.)

   Solution: Since $N(a + b\sqrt{10}) = a^2 - 10b^2 \equiv a^2 \pmod 5$, $N(a + b\sqrt{10}) \in \{[0], [1], [4]\}$ (mod 5). Hence $N(\alpha) \neq \pm 2, \pm 3$. ■

4. 3 is an irreducible element in R.

   Solution: Since $N(3) = 9$, and there is no element $\alpha \in R$ such that $N(\alpha) = \pm 3$, 3 is a primitive element. Note that if $3 = \alpha \cdot \beta$, then $9 = N(3) = N(\alpha)N(\beta)$, $N(\alpha) = \pm 1$ or $N(\beta) = \pm 1$. and $\alpha \in U(R)$ or $\beta \in U(R)$. ■

5. R is not a UFD. (Hint: Check whether $I = \langle 3 \rangle$ is a prime ideal or not.)

   Solution: Note that $(1+\sqrt{10})(1-\sqrt{10}) = -9 \in (3)$. If $1 \pm \sqrt{10} \in (3)$, then $1 \pm \sqrt{10} = 3 \cdot \alpha$ and $-9 = N(1 \pm \sqrt{10}) = N(3 \cdot \alpha) = N(3)N(\alpha) = 9 \cdot N(\alpha)$. Thus $\alpha \in U(R)$ and $(1 \pm \sqrt{10})/3 \in R$, which is absurd. Hence I is not a prime ideal. Therefore, R cannot be a UFD. ■

Quiz 8

Due: 10:00 a.m. November 13, 2006

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

Let $\alpha = \sqrt[3]{2} \in \boldsymbol{R}$, $p(t) = t^3 - 2 \in \boldsymbol{Q}[t]$ and $R = \boldsymbol{Q}[\alpha] = \{f(\alpha) \mid f(t) \in \boldsymbol{Q}[t]\}$. Show the following.

1. $p(t)$ is irreducible over $\boldsymbol{Q}$, i.e., it is irreducible as a polynomial in $\boldsymbol{Q}[t]$.

2. $\langle p(t) \rangle$ is a maximal ideal in $\boldsymbol{Q}[t]$.

3. $\boldsymbol{Q}[t]/\langle p(t) \rangle \simeq R$ and that R is a field.

4. $R = \{a_0 + a_1\alpha + a_2\alpha^2 \mid a_0, a_1, a_2 \in \boldsymbol{Q}\}$.

5. Find the multiplicative inverse of $1 + \alpha$ and express it in the form $a_0 + a_1\alpha + a_2\alpha^2$, where $a_0, a_1, a_2 \in \boldsymbol{Q}$.

Message: Requests? Questions?

Solutions to Quiz 8

November 13, 2006

Let $\alpha = \sqrt[3]{2} \in \boldsymbol{R}$, $p(t) = t^3 - 2 \in \boldsymbol{Q}[t]$ and $R = \boldsymbol{Q}[\alpha] = \{f(\alpha) \mid f(t) \in \boldsymbol{Q}[t]\}$. Show the following.

1. $p(t)$ is irreducible over $\boldsymbol{Q}$, i.e., it is irreducible as a polynomial in $\boldsymbol{Q}[t]$.

   Solution: Since $\boldsymbol{Z}$ is a UFD, we can apply (7.4.9) to $p(t) \in \boldsymbol{Z}[t]$ with $p = 2$. Note that $2 \mid -2 = a_0$, $2 \mid 0 = a_1 = a_2$ and that $2 \nmid 1 = a_3$, $2^2 \nmid -2 = a_0$. Thus $p(t)$ is irreducible over $\boldsymbol{Z}$. Since $\boldsymbol{Q}$ is the field of fractions of $\boldsymbol{Z}$, $p(t)$ is irreducible over $\boldsymbol{Q}$ by Gauss' Lemma (7.3.7). ■

2. $\langle p(t)\rangle$ is a maximal ideal in $\boldsymbol{Q}[t]$.

   Solution: Since $\boldsymbol{Q}$ is a field, $\boldsymbol{Q}[t]$ is a Euclidian domain by (7.1.3). Since every Euclidean domain is a principal ideal domain by (7.2.1), $\boldsymbol{Q}[t]$ is a principal ideal domain. Since $U(\boldsymbol{Q}[t]) = \boldsymbol{Q} \setminus \{0\}$, every irreducible polynomial in $\boldsymbol{Q}[t]$ is an irreducible element in $\boldsymbol{Q}[t]$. In particular, $p(t)$ is an irreducible element in $\boldsymbol{Q}[t]$. Thus by (7.2.6), the ideal generated by an irreducible element $p(t)$ is a maximal ideal in the principal ideal domain $\boldsymbol{Q}[t]$. ■

3. $\boldsymbol{Q}[t]/\langle p(t)\rangle \simeq R$ and that R is a field.

   Solution: Let $\theta_\alpha : \boldsymbol{Q}[t] \to \boldsymbol{C}$ $(f(t) \mapsto f(\alpha))$. Then clearly θ_α is a ring homomorphism and its image is R. Since $\boldsymbol{Q}[t]$ is a principal ideal domain, and $\mathrm{Ker}(\theta_\alpha)$ is an ideal, there exists a polynomial $q(t) \in \boldsymbol{Q}[t]$ such that $\mathrm{Ker}(\theta_\alpha) = \langle q(t)\rangle$. Since $p(\alpha) = \alpha^3 - 2 = 0$, $p(t) \in \mathrm{Ker}(\theta_\alpha) = \langle q(t)\rangle$ and $q(t) \mid p(t)$. Since $q(t) \in \mathrm{Ker}(\theta_\alpha)$, $q(t)$ is not a constant. Since $p(t)$ is irreducible, $p(t)$ is a nonzero constant multiple of $q(t)$. Thus $\mathrm{Ker}(\theta_\alpha) = \langle q(t)\rangle = \langle p(t)\rangle$. Now by First Isomorphism Theorem (6.2.4), $\boldsymbol{Q}[t]/\langle p(t)\rangle = \boldsymbol{Q}[t]/\langle p(t)\rangle \simeq \mathrm{Im}(\theta_\alpha) = R$, as desired. ■

4. $R = \{a_0 + a_1\alpha + a_2\alpha^2 \mid a_0, a_1, a_2 \in \boldsymbol{Q}\}$.

   Solution: Let $f(t) \in \boldsymbol{Q}[t]$. By (7.1.3), there exists $q(t)$ and $r(t) \in \boldsymbol{Q}[t]$ such that $f(t) = q(t)p(t) + r(t)$ with $\deg(r(t)) < \deg(p(t)) = 3$. Since $p(\alpha) = 0$, $f(\alpha) = r(\alpha)$. Therefore, $f(\alpha) = r(\alpha) \in \{a_0 + a_1\alpha + a_2\alpha^2 \mid a_0, a_1, a_2 \in \boldsymbol{Q}\}$, as the degree of $r(t)$ is at most 2. This proves $R \subset \{a_0 + a_1\alpha + a_2\alpha^2 \mid a_0, a_1, a_2 \in \boldsymbol{Q}\}$. The other inclusion is clear by definition. ■

5. Find the multiplicative inverse of $1 + \alpha$ and express it in the form $a_0 + a_1\alpha + a_2\alpha^2$, where $a_0, a_1, a_2 \in \boldsymbol{Q}$.

   Solution: Let $\omega = (-1 + \sqrt{-3})/2$. Then $1 + \omega + \omega^2 = 0$ and $\omega^3 = 1$. Now compute

   $$(1+\alpha)(1+\alpha\omega)(1+\alpha\omega^2) = 1 + \alpha(1+\omega+\omega^2) + \alpha^2(1+\omega+\omega^2) + \alpha^3 = 3.$$

   Hence

   $$(1+\alpha)^{-1} = \frac{1}{3}(1+\alpha\omega)(1+\alpha\omega^2) = \frac{1}{3}(1+\alpha(\omega+\omega^2)+\alpha^2) = \frac{1}{3}(1-\alpha+\alpha^2).$$

   Therefore $a_0 = 1/3$, $a_1 = -1/3$ and $a_2 = 1/3$. ■