Quiz 1

(*Due Wednesday, December 12, 2007*)

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

Let F be a field and $F[t]$ the polynomial ring over F. Then for $f, g \in F[t]$ with $g \neq 0$, there exist $q, r \in F[t]$ such that

$$f = q \cdot g + r, \text{ with } \deg r < \deg g. \tag{1}$$

Use this fact and prove the following. Note that $g \mid f$ if and only if $r = 0$ in (1).

1. Let $f \in F[t]$ and $a \in F$. Then $f(a) = 0 \Leftrightarrow t - a \mid f$.

2. Let I be an ideal of $F[t]$. Then there exists $p \in F[t]$ such that $I = (p) = \{g \cdot p \mid g \in F[t]\}$.

3. Let $I = (p)$ be an ideal of $F[t]$ generated by $p \in F[t]$. Then I is a maximal ideal if and only if p is irreducible.

4. Let $I = (p) \neq \{0\}$ be a *nonzero* ideal of $F[t]$ generated by $p \in F[t]$. Then I is a prime ideal if and only if p is irreducible.

Message: Questions? Suggestions?

Solutions to Quiz 1

1. Let $f \in F[t]$ and $a \in F$. Then $f(a) = 0 \Leftrightarrow t - a \mid f$.

   Sol. By the division algorithm above, there exists $q \in F[t]$ such that

   $$f = q \cdot (t - a) + r, \text{ with} \deg r < \deg(t - a) = 1.$$

   Hence r is a constant and $r \in F$. Since $f(a) = r$, $f(a) = 0$ if and only if $r = 0$, i.e., $(t - a) \mid f$. ■

2. Let I be an ideal of $F[t]$. Then there exists $p \in F[t]$ such that $I = (p) = \{g \cdot p \mid g \in F[t]\}$.

   Sol. If $I = \{0\}$, then we can take $p = 0$. Hence we may assume that $I \neq \{0\}$. Let p be a nonzero element of I such that $\deg p$ is minumum. Let $f \in I$. Then there exists $q, r \in F[t]$ such that $f = q \cdot p + r$ with $\deg r < \deg p$. Since $r = f - q \cdot p \in I$ and $\deg r < \deg p$, $r = 0$ by the choice of p. Hence $f = q \cdot p$ and $f \in (p)$. Thus $I \subset (p)$. Since $p \in I$, the other inclusion is obvious.

   An integral domain with this property is called a principal ideal domain (PID). Every Euclidean domain is a PID. Hence the statebment above follows from the fact that $F[t]$ is an Euclidean domain, which is stated in the begining of this quiz. ■

3. Let $I = (p)$ be an ideal of $F[t]$ generated by $p \in F[t]$. Then I is a maximal ideal if and only if p is irreducible.

   Sol. Let J be an ideal containing $I = (p)$. Then by 2, there exists $q \in J$ such that $J = (q)$. Hence there exists $g \in F[t]$ such that $p = g \cdot q$. Now assume that p is irreducible. Then either g or q is a unit, i.e., a nonzero constant. Hence $J = (q) = (g \cdot q) = (p) = I$ if g is a unit, and $J = (q) = F[t]$ if q is a unit. Hence I is a maximal ideal. Suppose I is a maximal ideal. If $p = g \cdot q$ for some $g, q \in F[t]$, then $(p) \subseteq (q)$. Hence either $(p) = (q)$ or $(q) = F[t]$ and q is a unit. If $(p) = (q)$, then g is a unit. Therefore, p is irreducible.

   For a nonzero ideal I of a PID, let $I = (p)$. Then the following three properties are equivalent; (i) I is maximal, (ii) I is prime, and (iii) p is irreducible. $F[t]$ is a PID and p is irreducible in $F[t]$ if and only if p is an irreducible polynomial. Note that for a commutative ring R, R is an integral domain, if and only if (0) is a prime ideal. Hence in the next problem, we need the assumption that $I \neq (0)$. ■

4. Let $I = (p) \neq \{0\}$ be a *nonzero* ideal of $F[t]$ generated by $p \in F[t]$. Then I is a prime ideal if and only if p is irreducible.

   Sol. If p is irreducible, then I is a maximal ideal by 3 and I is a prime ideal. Suppose I is a prime ideal and $p = g \cdot q$ for some $g, q \in F[t]$. Since $p \in I$, and I is a prime ideal, $g \in (p)$ or $q \in (p)$. That is either $p \mid g$ or $p \mid q$. We have either q or g is a unit. ■

Quiz 2

(*Due on Wednesday December 19, 2007*)

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

Let $m \geq 2$ be a positive integer such that $p \mid m \Rightarrow p^2 \nmid m$ for every prime number p. (e.g., $m = 2, 3, 5, 6, 7, 10, 11, 13, 14, 15, \ldots$.) Let n be another positive integer.

1. Show that $f(t) = t^n - m \in \boldsymbol{Q}[t]$ is irreducible over $\boldsymbol{Q}$.

2. Let $\alpha = \sqrt[n]{m} \in \boldsymbol{R}$. Show that $(\boldsymbol{Q}(\alpha) : \boldsymbol{Q}) = n$.

3. Let $\beta = \sqrt[3]{6} \in \boldsymbol{R}$. Show that $\boldsymbol{Q}(\beta) = \{a + b\beta + c\beta^2 \mid a, b, c \in \boldsymbol{Q}\}$.

4. Let β be above. Express $(1 + \beta)^{-1}$ as $a + b\beta + c\beta^2$ with $a, b, c \in \boldsymbol{Q}$.

5. Suppose α, β be as above and $3 \nmid n$. Show that $(\boldsymbol{Q}(\alpha, \beta) : \boldsymbol{Q}) = 3n$.

Message: 何でもどうぞ。

Solutions to Quiz 2

Let $m \geq 2$ be a positive integer such that $p \mid m \Rightarrow p^2 \nmid m$ for every prime number p. (e.g., $m = 2, 3, 5, 6, 7, 10, 11, 13, 14, 15, \ldots$.) Let n be another positive integer.

1. Show that $f(t) = t^n - m \in \boldsymbol{Q}[t]$ is irreducible over $\boldsymbol{Q}$.

   Sol. Since $m \geq 2$, there is a prime which divides m. By assumption, $p^2 \nmid m$. Hence by Eisenstein's criterion and Gauss' lemma $f(t)$ is irreducible over $\boldsymbol{Q}$. ■

2. Let $\alpha = \sqrt[n]{m} \in \boldsymbol{R}$. Show that $(\boldsymbol{Q}(\alpha) : \boldsymbol{Q}) = n$.

   Sol. $f(t) = t^n - m$ is the minimum polynomial of α. Hence $(\boldsymbol{Q}(\alpha) : \boldsymbol{Q}) = \deg f(t) = n$. (That is $f(\alpha) = 0$ and if $g(\alpha) = 0$ for some $g(t) \in \boldsymbol{Q}[t]$ then $f(t) \mid g(t)$. If $p(t) \in \boldsymbol{Q}[t]$ is a monic polynomial minimum degree such that $p(\alpha) = 0$, and $f(t) = q(t)p(t) + r(t)$ with $\deg(r(t)) < \deg(p(t))$. Then $r(\alpha) = 0$ and $r(t) = 0$ by the choice of $g(t)$. Hence $f(t) = q(t)p(t)$. Since $f(t)$ is irreducible, $q(t) = 1$ as the leading coefficients of p and f are 1. Hence $f(t) = p(t)$ and $g(\alpha) = 0$ implies $f(t) \mid g(t)$. Consider a ring homomorphism $\phi : \boldsymbol{Q}[t] \to \boldsymbol{R}(g(t) \mapsto g(\alpha))$. Then $\ker(\phi) = (f(t))$ and $\mathrm{im}(\phi) = \boldsymbol{Q}(\alpha)$. Hence $\boldsymbol{Q}[t]/(f(t)) \simeq \boldsymbol{Q}(\alpha)$. $\boldsymbol{Q}[t]/(f(t)) = \{a + bt + ct^2 + (f(t)) \mid a, b, c \in \boldsymbol{Q}\}$.) Please review Proposition 2.2 (10.1.5). ■

3. Let $\beta = \sqrt[3]{6} \in \boldsymbol{R}$. Show that $\boldsymbol{Q}(\beta) = \{a + b\beta + c\beta^2 \mid a, b, c \in \boldsymbol{Q}\}$.

   Sol. Apply the previous problem to β. $1, \beta, \beta^2$ are linearly independent as otherwise there is a polynomial of degree at most two in $\boldsymbol{Q}[t]$ such that β is a root of it. ■

4. Let β be above. Express $(1+\beta)^{-1}$ as $a + b\beta + c\beta^2$ with $a, b, c \in \boldsymbol{Q}$.

   Sol. Since $\beta^3 - 6 = 0$,

$$(1+\beta)^{-1} = \frac{7}{7(1+\beta)} = \frac{1+\beta^3}{7(1+\beta)} = \frac{1-\beta+\beta^2}{7} = \frac{1}{7} - \frac{1}{7}\beta + \frac{1}{7}\beta^2.$$

5. Suppose α, β be as above and $3 \nmid n$. Show that $(\boldsymbol{Q}(\alpha, \beta) : \boldsymbol{Q}) = 3n$.

   Sol. $(\boldsymbol{Q}(\alpha,\beta) : \boldsymbol{Q}) = (\boldsymbol{Q}(\alpha,\beta) : \boldsymbol{Q}(\alpha))(\boldsymbol{Q}(\alpha) : \boldsymbol{Q})$. So this number is divisible by n. Since $\boldsymbol{Q}(\beta) \subseteq \boldsymbol{Q}(\alpha, \beta)$, it is also divisible by $3 = (\boldsymbol{Q}(\beta) : \boldsymbol{Q})$. Since $3 \nmid n$, $(\boldsymbol{Q}(\alpha, \beta) : \boldsymbol{Q}) = 3n$. ■

Quiz 3

(*Due on Wednesday January 9, 2008*)

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

1. Trisect the given angle $\frac{\pi}{4}$ by ruler and compass.

2. Show that it is impossible to draw a regular 9-gon by ruler and compass.

3. Draw a regular pentagon (5-gon) by ruler and compass. (Hint: Find a root of $t^4 + t^3 + t^2 + t + 1 = 0$ by setting $u = t + \frac{1}{t}$, and consider its geometrical meaning in the complex plane.)

Message: 何でもどうぞ。

Solutions to Quiz 3

1. Trisect the given angle $\frac{\pi}{4}$ by ruler and compass.

   Sol. Suppose that the angle is given by two line segments intersecting at the origin. Draw a circle with center at the origin. Let A and B be two points of intersection. Draw a right dodecagon (12-gon) such that one of the vertex is at A. This gives a point trisecting the angle. A right dodecagon can be easily drawn as it can be obtained from a equilateral triangle by bisecting it twice. ■

2. Show that it is impossible to draw a regular 9-gon by ruler and compass.

   Sol. Let $\alpha = 2\pi/3$. Then $\cos\alpha = -1/2$. Hence $\boldsymbol{Q}(\cos\alpha) = \boldsymbol{Q}$. Let $\theta = \alpha/3$. If it is possible to draw a regular 9-gon, then θ is constructible. Let

   $$f(t) = 8t^3 - 6t + 1.$$

   It suffices to show that $f(t)$ is reducible over $\boldsymbol{Q}$ (10.2.4). Let $g(u) = u^3 f(1/u) = u^3 - 6u^2 + 8$. By Gauss' lemma, if $g(u)$ is reducible, one of $\pm1, \pm2, \pm4, \pm8$ is a root, which is not the case. Hence $f(t)$ is irreducible as well. Or consider $f(t)$ modulo 7. Then it becomes $t^3 + t + 1$. This polynomial does not have a root in $\boldsymbol{Z}_7$. Hence it is irreducible over $\boldsymbol{Z}_7$, so $f(t)$ is irreducible over $\boldsymbol{Q}$. ■

3. Draw a regular pentagon (5-gon) by ruler and compass. (Hint: Find a root of $t^4 + t^3 + t^2 + t + 1 = 0$ by setting $u = t + \frac{1}{t}$, and consider its geometrical meaning in the complex plane.)

   Sol.

   $$0 = t^4 + t^3 + t^2 + t + 1 = t^2(t^2 + 2 + \frac{1}{t^2} + t + \frac{1}{t} - 1) = t^2(u^2 + u - 1)$$

   If we set

   $$\theta = \cos\frac{2\pi}{5} + \sqrt{-1}\sin\frac{2\pi}{5},$$

   then the roots of $t^4 + t^3 + t^2 + t + 1 = 0$ is $\theta, \theta^2, \theta^3, \theta^4$ and $\theta^5 = 1$. So

   $$u = t + \frac{1}{t} = \theta + \theta^4 = 2\cos\frac{2\pi}{5} > 0 \text{ or } \theta^2 + \theta^3 = 2\cos\frac{4\pi}{5} < 0.$$

   Therefore

   $$2\cos\frac{2\pi}{5} = \frac{-1+\sqrt{5}}{2} \text{ or } \cos\frac{2\pi}{5} = \frac{-1+\sqrt{5}}{4}.$$

   Now starting from a unit circle, it is easy to construct θ.

   See http://www.geocities.jp/two_well/penta.kakikata.html

Quiz 4

(*Due on Monday January 21, 2008*)

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

Let $p(t) = t^2 + 1$, $q(t) = t^2 + t + 2$ and $r(t) = t^2 + 2 \in \boldsymbol{Z}_3[t]$.

1. Show that $p(t)$ and $q(t)$ are irreducible over $\boldsymbol{Z}_3$.

2. Factor $t^9 - t \in \boldsymbol{Z}_3[t]$.

3. Let $p(t) = t^2 + 1$. Write the multiplication table of $\boldsymbol{Z}_3[t]/(p(t))$ with respect to the product.

4. Show that $\boldsymbol{Z}_3[t]/(p(t)) \simeq \boldsymbol{Z}_3[t]/(q(t))$.

5. Determine whether or not $\boldsymbol{Z}_3[t]/(p(t)) \simeq \boldsymbol{Z}_3[t]/(r(t))$.

Message: 何でもどうぞ。

Solutions to Quiz 4

(*January 21, 2008*)

Let $p(t) = t^2 + 1$, $q(t) = t^2 + t + 2$ and $r(t) = t^2 + 2 \in \boldsymbol{Z}_3[t]$.

1. Show that $p(t)$ and $q(t)$ are irreducible over $\boldsymbol{Z}_3$.

   Sol. Suppose not. Then it must have a linear factor, or equivalently it has a root in $\boldsymbol{Z}_3 = \{0, 1, -1\}$. Since $p(0) = 1$, $p(1) = p(-1) = 2 = -1$ and $q(0) = 2$, $q(1) = 1$ and $q(-1) = 2 = -1$, it is not the case. ■

2. Factor $t^9 - t \in \boldsymbol{Z}_3[t]$.

   Sol.
   $$t^9 - t = t(t-1)(t+1)(t^2+1)(t^2+t+2)(t^2+2t+2)$$
   Note that the factors above are all the monic irreducible polynomials of degree at most 2. ■

3. Let $p(t) = t^2 + 1$. Write the multiplication table of $\boldsymbol{Z}_3[t]/(p(t))$ with respect to the product.

   Sol. All elements are represented by polynomials of degree at most 1. Hence

	0	1	$t+1$	$-t$	$-t+1$	-1	$-t-1$	t	$t-1$
0	0	0	0	0	0	0	0	0	0
1	0	1	$t+1$	$-t$	$-t+1$	-1	$-t-1$	t	$t-1$
$t+1$	0	$t+1$	$-t$	$-t+1$	-1	$-t-1$	t	$t-1$	1
$(t+1)^2 = -t$	0	$-t$	$-t+1$	-1	$-t-1$	t	$t-1$	1	$t+1$
$(t+1)^3 = -t+1$	0	$-t+1$	-1	$-t-1$	t	$t-1$	1	$t+1$	$-t$
$(t+1)^4 = -1$	0	-1	$-t-1$	t	$t-1$	1	$t+1$	$-t$	$-t+1$
$(t+1)^5 = -t-1$	0	$-t-1$	t	$t-1$	1	$t+1$	$-t$	$-t+1$	-1
$(t+1)^6 = t$	0	t	$t-1$	1	$t+1$	$-t$	$-t+1$	-1	$-t-1$
$(t+1)^7 = t-1$	0	$t-1$	1	$t+1$	$-t$	$-t+1$	-1	$-t-1$	t

4. Show that $\boldsymbol{Z}_3[t]/(p(t)) \simeq \boldsymbol{Z}_3[t]/(q(t))$.

   Sol. Since both $p(t)$ and $q(t)$ are irreducible, $\boldsymbol{Z}_3[t]/(p(t))$ and $\boldsymbol{Z}_3[t]/(q(t))$ are fields of order 9. Hence they are isomorphic. Can you find an isomorphism between them? (How about $t \mapsto t-1$? What is the minimal polynomial of $t-1+(q(t)) \in \boldsymbol{Z}_3[t]/(q(t))$ over $\boldsymbol{Z}_3$?) ■

5. Determine whether or not $\boldsymbol{Z}_3[t]/(p(t)) \simeq \boldsymbol{Z}_3[t]/(r(t))$.

   Sol. Since $r(1) = 0$, $r(t) = (t-1)(t+1)$ is not irreducible, $\boldsymbol{Z}_3[t]/(r(t))$ is not a field. So they are not isomorphic. In fact, $t - 1 + (r(t)) \neq 0$, $t + 1 + (r(t)) \neq 0$ in $\boldsymbol{Z}_3[t]/(r(t))$ but the product is zero. ■

Quiz 5

(*Due on January 28, 2008*)

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

Let n be an integer such that $n > 2$ and $\zeta = e^{2\pi\sqrt{-1}/n} = \cos(2\pi/n) + \sqrt{-1}\sin(2\pi/n)$.

1. Let $F \subset E$ be a field extension. Let x be a nonzero algebraic element of E over F and $f = \mathrm{Irr}_F(x)$. If $g \in F[t]$ has x as its root, i.e., $g(x) = 0$, then f divides g.

2. Let $f = \mathrm{Irr}_{\boldsymbol{Q}}(\zeta)$. Show that $\zeta^n = 1$ and every root of f is a power of ζ.

3. Show that $\boldsymbol{Q}(\zeta)$ is normal over $\boldsymbol{Q}$.

4. Show that $\boldsymbol{Q}(\sqrt[n]{2})$ is not normal over $\boldsymbol{Q}$.

5. Show that $\boldsymbol{Q}(\sqrt[n]{2}, \zeta)$ is normal over $\boldsymbol{Q}$.

Message: 何でもどうぞ。

Solutions to Quiz 5

(*January 28, 2008*)

Let n be an integer such that $n > 2$ and $\zeta = e^{2\pi\sqrt{-1}/n} = \cos(2\pi/n) + \sqrt{-1}\sin(2\pi/n)$.

1. Let $F \subset E$ be a field extension. Let x be a nonzero algebraic element of E over F and $f = \mathrm{Irr}_F(x)$. If $g \in F[t]$ has x as its root, i.e., $g(x) = 0$, then f divides g.

   Sol. Since $f \neq 0$, there exists $q, r \in F[t]$ with $\deg r < \deg f$ such that $g = qf + r$. Since $0 = g(x) = q(x)f(x) + r(x) = r(x)$ and $\deg r < \deg f$, $r = 0$. Hence f divides g. ■

2. Let $f = \mathrm{Irr}_{\boldsymbol{Q}}(\zeta)$. Show that $\zeta^n = 1$ and every root of f is a power of ζ.

   Sol. Let $g = t^n - 1$. Then by Problem 1, $f \mid g$. Hence every root of f is a root of g. On the other hand $1, \zeta, \ldots, \zeta^{n-1}$ are distinct roots of g. Since $\deg g = n$, these are the all roots of g. Hence every root of f is a power of ζ. ■

3. Show that $\boldsymbol{Q}(\zeta)$ is normal over $\boldsymbol{Q}$.

   Sol. $\boldsymbol{Q}(\zeta)$ is a splitting field of $t^n - 1$ over $\boldsymbol{Q}$. Hence it is normal over $\boldsymbol{Q}$ by (11.1.1). ■

4. Show that $\boldsymbol{Q}(\sqrt[n]{2})$ is not normal over $\boldsymbol{Q}$.

   Sol. By Eisenstein's criterion and Gauss' lemma, $t^n - 2$ is irreducible over $\boldsymbol{Q}$ and $\boldsymbol{Q}(\sqrt[n]{2})$ contains its root $\sqrt[n]{2}$. On the other hand, the roots of $t^n - 2$ are $\sqrt[n]{2}, \sqrt[n]{2}\zeta, \ldots, \sqrt[n]{2}\zeta^{n-1}$ and $\zeta \notin \boldsymbol{R}$ as $n > 2$, $\boldsymbol{Q}(\sqrt[n]{2}) \subset \boldsymbol{R}$ cannot contain all roots of $t^n - 2$. ■

5. Show that $\boldsymbol{Q}(\sqrt[n]{2}, \zeta)$ is normal over $\boldsymbol{Q}$.

   Sol. Clearly $t^n - 2$ splits in the field $\boldsymbol{Q}(\sqrt[n]{2}, \zeta)$. Let K be the splitting field of $t^n - 2$ contained in $\boldsymbol{Q}(\sqrt[n]{2}, \zeta)$. Then $\sqrt[n]{2} \in K$ and $\sqrt[n]{2}\zeta \in K$. Hence $\zeta \in K$. Therefore $K = \boldsymbol{Q}(\sqrt[n]{2}, \zeta)$. ■

Quiz 6

(*Due on February 4, 2008*)

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

Let $E = \boldsymbol{Q}(\sqrt[4]{2}, \sqrt{-1}) \subset \boldsymbol{C}$ and $K = \boldsymbol{Q}(\sqrt[4]{2})$ and $F = \boldsymbol{Q}(\sqrt{-1})$. Let $f = t^4 - 2 \in \boldsymbol{Q}[t]$.

1. Show that E is the splitting field of f over $\boldsymbol{Q}$ contained in $\boldsymbol{C}$.

2. Show that $(E : \boldsymbol{Q}) = 8$.

3. Let σ be the complex conjugate, i.e., $\sigma : \boldsymbol{C} \to \boldsymbol{C}\ (a + b\sqrt{-1} \mapsto a - b\sqrt{-1},\ a, b \in \boldsymbol{R})$. Show that $\sigma(E) = E$ and $\alpha = \sigma_{|E} : E \to E$ belongs to $\mathrm{Gal}(E/K)$.

4. Show that there is an element $\beta \in \mathrm{Gal}(E/F)$ such that $\beta(\sqrt[4]{2}) = \sqrt[4]{2}\sqrt{-1}$.

5. Find the order of $\mathrm{Gal}(E/\boldsymbol{Q})$.

Message: 何でもどうぞ。

Solutions to Quiz 6 *(February 4, 2008)*

Let $E = \boldsymbol{Q}(\sqrt[4]{2}, \sqrt{-1}) \subset \boldsymbol{C}$ and $K = \boldsymbol{Q}(\sqrt[4]{2})$ and $F = \boldsymbol{Q}(\sqrt{-1})$. Let $f = t^4 - 2 \in \boldsymbol{Q}[t]$.

1. Show that E is the splitting field of f over $\boldsymbol{Q}$ contained in $\boldsymbol{C}$.

   Sol. The roots of f are $\pm\sqrt[4]{2}, \pm\sqrt[4]{2}\sqrt{-1}$. Hence $t^4 - 2$ splits in E. On the other hand, $\boldsymbol{Q}(\sqrt[4]{2}, -\sqrt[4]{2}, \sqrt[4]{2}\sqrt{-1}, -\sqrt[4]{2}\sqrt{-1}) = \boldsymbol{Q}(\sqrt[4]{2}, \sqrt{-1}) = E$. ■

2. Show that $(E : \boldsymbol{Q}) = 8$.

   Sol. Since all elements of K are real, $t^2 + 1$ is irreducible over K. Hence

   $$(E, \boldsymbol{Q}) = (E, K)(K, \boldsymbol{Q}) = (K(\sqrt{-1}), K)(\boldsymbol{Q}(\sqrt[4]{2} : \boldsymbol{Q}) = \deg(t^2+1)\deg(t^4-2) = 2\cdot 4 = 8.$$

3. Let σ be the complex conjugate, i.e., $\sigma : \boldsymbol{C} \to \boldsymbol{C}\,(a + b\sqrt{-1} \mapsto a - b\sqrt{-1},\ a, b \in \boldsymbol{R})$. Show that $\sigma(E) = E$ and $\alpha = \sigma_{|E} : E \to E$ belongs to $\mathrm{Gal}(E/K)$.

   Sol. Clearly σ is an automorphism of $\boldsymbol{C}$, $\sigma_{|\boldsymbol{Q}} = id$ and $\sigma(\sqrt[4]{2}) = \sqrt[4]{2}$. Moreover $\sigma(\sqrt{-1}) = -\sqrt{-1}$. Hence $\sigma(E) \subset E$. Since $(\sigma(E), \boldsymbol{Q}) = (E : \boldsymbol{Q}) < \infty$, by a property of finite dimensional linear space, $\sigma(E) = E$. Since $K \subset \boldsymbol{R}$, we have $\beta \in \mathrm{Gal}(E/K)$. ■

4. Show that there is an element $\beta \in \mathrm{Gal}(E/F)$ such that $\beta(\sqrt[4]{2}) = \sqrt[4]{2}\sqrt{-1}$.

   Sol. Since $E = F(\sqrt[4]{2})$, $(E : \boldsymbol{Q}) = 8$ and $(F : \boldsymbol{Q}) = 2$, $(E : F) = 4 = \deg(\mathrm{Irr}_F(\sqrt[4]{2}))$. We have $t^4 - 2 = \mathrm{Irr}_F(\sqrt[4]{2})$. Hence by (10.3.2), id_F can be extended to $\beta \in \mathrm{Gal}(E/F)$ such that $\beta(\sqrt[4]{2}) = \sqrt[4]{2}\sqrt{-1}$. Note that $F(\sqrt[4]{2}) = E = F(\sqrt[4]{2}\sqrt{-1})$. ■

5. Find the order of $\mathrm{Gal}(E/\boldsymbol{Q})$.

   Sol. Since the characteristic of E is zero, the extension $E/\boldsymbol{Q}$ is separable. Since E is a splitting field of f, it is normal. Therefor it is Galois and by (11.2.2), $|\mathrm{Gal}(E/\boldsymbol{Q})| = (E : \boldsymbol{Q}) = 8$.

   We can list all elements of $\mathrm{Gal}(E/\boldsymbol{Q})$ as well. Be careful that we need to show that all are distinct.

Quiz 7

(*Due on February 13, 2008*)

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

Let $E = \boldsymbol{Q}(\sqrt[4]{2}, \sqrt{-1}) \subset \boldsymbol{C}$ and $K = \boldsymbol{Q}(\sqrt[4]{2})$ and $F = \boldsymbol{Q}(\sqrt{-1})$. Let $f = t^4 - 2 \in \boldsymbol{Q}[t]$. Let σ be the complex conjugate and $\beta \in \mathrm{Gal}(E/F)$ defined in Quiz 6.

1. Show that $\sigma\beta\sigma = \beta^{-1}$.

2. $\mathrm{Gal}(E/\boldsymbol{Q}) = \{1, \beta, \beta^2, \beta^3, \sigma, \sigma\beta, \sigma\beta^2, \sigma\beta^3\}$.

3. Find $\mathrm{Fix}(\langle\sigma\rangle)$.

4. Find $\mathrm{Fix}(\langle\beta\rangle)$.

5. Find $\mathrm{Fix}(\langle\sigma\beta\rangle)$.

Message: 何でもどうぞ。

Solutions to Quiz 7

(*February 13, 2008*)

Let $E = \boldsymbol{Q}(\sqrt[4]{2}, \sqrt{-1}) \subset \boldsymbol{C}$ and $K = \boldsymbol{Q}(\sqrt[4]{2})$ and $F = \boldsymbol{Q}(\sqrt{-1})$. Let $f = t^4 - 2 \in \boldsymbol{Q}[t]$. Let σ be the complex conjugate and $\beta \in G = \mathrm{Gal}(E/F)$ defined in Quiz 6.

1. Show that $\sigma\beta\sigma = \beta^{-1}$.

   Sol. Since $E = \boldsymbol{Q}(\sqrt[4]{2}, \sqrt{-1})$, it is sufficient to show that $\sigma\beta\sigma\beta(\sqrt[4]{2}) = \sqrt[4]{2}$ and $\sigma\beta\sigma\beta(\sqrt{-1}) = \sqrt{-1}$.

$$\sigma\beta\sigma\beta(\sqrt[4]{2}) = \sigma\beta\sigma(\sqrt[4]{2}\sqrt{-1}) = \sigma\beta(-\sqrt[4]{2}\sqrt{-1}) = \sigma(\sqrt[4]{2}) = \sqrt[4]{2}.$$

$$\sigma\beta\sigma\beta(\sqrt{-1}) = \sigma\beta\sigma(\sqrt{-1}) = \sigma\beta(-\sqrt{-1}) = \sigma(-\sqrt{-1}) = \sqrt{-1}.$$

2. $\mathrm{Gal}(E/\boldsymbol{Q}) = \{1, \beta, \beta^2, \beta^3, \sigma, \sigma\beta, \sigma\beta^2, \sigma\beta^3\}$.

   Sol. Since $\beta(\sqrt[4]{2}) = \sqrt[4]{2}\sqrt{-1}$, $\beta(\sqrt[4]{2}\sqrt{-1}) = -\sqrt[4]{2}$, the order of β is four. The order of σ is two. Let $H = \langle \beta \rangle$. By 1, $H \triangleleft G$ and $(G : H) = 2$. Now we have the assertion. ∎

3. Find $\mathrm{Fix}(\langle \sigma \rangle)$.

   Sol. Since $(\boldsymbol{Q}(\sqrt[4]{2}) : \boldsymbol{Q}) = 4$ and $\boldsymbol{Q}(\sqrt[4]{2}) \subset \mathrm{Fix}(\langle \sigma \rangle)$,

$$2 = |\langle \sigma \rangle| = (E : \mathrm{Fix}(\langle \sigma \rangle)) \leq (E : \boldsymbol{Q}(\sqrt[4]{2})) = 2.$$

   Hence $\mathrm{Fix}(\langle \sigma \rangle) = \boldsymbol{Q}(\sqrt[4]{2}) = K$. ∎

4. Find $\mathrm{Fix}(\langle \beta \rangle)$.

   Sol. Since $(\boldsymbol{Q}(\sqrt{-1}) : \boldsymbol{Q}) = 2$ and $\boldsymbol{Q}(\sqrt{-1}) \subset \mathrm{Fix}(\langle \beta \rangle)$,

$$4 = |\mathrm{Fix}(\langle \beta \rangle)| = (E : \mathrm{Fix}(\langle \beta \rangle)) \leq (E : \boldsymbol{Q}(\sqrt{-1})) = 4.$$

   Hence $\mathrm{Fix}(\langle \beta \rangle) = \boldsymbol{Q}(\sqrt{-1}) = F$.

5. Find $\mathrm{Fix}(\langle \sigma\beta \rangle)$. ∎

   Sol. First note that

$$\sigma\beta(\sqrt[4]{2}(1-\sqrt{-1})) = \sigma(\sqrt[4]{2}\sqrt{-1}(1-\sqrt{-1})) = -\sqrt[4]{2}\sqrt{-1}(1+\sqrt{-1}) = \sqrt[4]{2}(1-\sqrt{-1}).$$

   Since $(\boldsymbol{Q}(\sqrt[4]{2}(1-\sqrt{-1})) : \boldsymbol{Q}) > 2$ and hence the index is four, and $\boldsymbol{Q}(\sqrt[4]{2}(1-\sqrt{-1})) \subset \mathrm{Fix}(\langle \sigma\beta \rangle)$,

$$2 = |\mathrm{Fix}(\langle \sigma\beta \rangle)| = (E : \mathrm{Fix}(\langle \sigma\beta \rangle)) \leq (E : \boldsymbol{Q}(\sqrt[4]{2}(1-\sqrt{-1}))) \leq 2$$

   Hence $\mathrm{Fix}(\langle \sigma\beta \rangle) = \boldsymbol{Q}(\sqrt[4]{2}(1-\sqrt{-1}))$. ∎

Quiz 8

(*Due on February 20, 2008*)

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

Let L be a finite Galois extension of F and $G = \mathrm{Gal}(L/F) = \langle \tau \rangle$ a cyclic group of order n generated by τ. The following function $N_{L/F}$ is called the norm function of the extension.

$$N = N_{L/F} : L \to L \ (a \mapsto N(a) = a \cdot \tau(a) \cdot \tau^2(a) \cdots \tau^{n-1}(a))$$

1. Let $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in L$. Show that if $\alpha_0 x + \alpha_1 \tau(x) + \cdots + \alpha_{n-1}\tau^{n-1}(x) = 0$ for all $x \in L$, then $\alpha_0 = \alpha_1 = \cdots = \alpha_{n-1} = 0$. (Hint: First take a shortest nonzero linear combination and use the fact that there is $y \in L$ such that $\tau(y) \neq y$.)

2. Show that $N(a) \in F$. (Hint: (11.2.6))

3. Suppose $a = b/\tau(b)$ for some $b \in L$. Show that $N(a) = 1$.

4. Let $a \in L$ and $N(a) = 1$. By 1, there is an element $c \in L$ such that

$$b = a\tau^0(c) + a\tau(a)\tau^1(c) + \cdots + (a\tau(a)\cdots\tau^{n-1}(a))\tau^{n-1}(c) \neq 0.$$

   Show that $a = b/\tau(b)$.

5. Suppose n is a prime and F contains a primitive n-th root of unity. Show that there is $a \in L$ such that $a^n \in F$ and $L = F(a)$.

Message: 何でもどうぞ。

Solutions to Quiz 8

(*February 20, 2008*)

1. Let $\alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in L$. Show that if $\alpha_0 x + \alpha_1 \tau(x) + \cdots + \alpha_{n-1}\tau^{n-1}(x) = 0$ for all $x \in L$, then $\alpha_0 = \alpha_1 = \cdots = \alpha_{n-1} = 0$.

   Sol. Among all nontrivial expressions, take the one such that the largest index i with $\alpha_i \neq 0$ is smallest. Let $y \in L$ such that $y \neq \tau(y)$. Then $y \neq 0$ and we have two equations.

   $$\begin{aligned} 0 &= \alpha_0 + \alpha_1 \tau(y)\tau(x) + \cdots + \alpha_{i-1}\tau^{i-1}(y)\tau^{i-1}(x) + \alpha_i \tau^i(y)\tau^i(x) \\ 0 &= \alpha_0 \tau^i(y) + \alpha_1 \tau^i(y)\tau(x) + \cdots + \alpha_i \tau^i(y)\tau^{i-1}(x) + \alpha_i \tau^i(y)\tau^i(x). \end{aligned}$$

   Taking the difference we have

   $$\begin{aligned} 0 &= \alpha_0(\tau^i(y) - 1) + \alpha_1(\tau^i(y) - \tau(y))\tau(x) + \cdots + \alpha_{i-1}(\tau^i(y) - \tau^{i-1}(y))\tau^{i-1}(x) \\ &= \alpha_0(\tau^i(y) - 1) + \alpha_1(\tau^i(y) - \tau(y))\tau(x) + \cdots + \alpha_{i-1}\tau^{i-1}(y)(\tau(y) - 1)\tau^{i-1}(x). \end{aligned}$$

   Since the equation holds for all $x \in L$, and we have a shorter expression. This is a contradiction and we have the assertion.

2. Show that $N(a) \in F$. (Hint: (11.2.6))

   Sol.

   $$\tau(N(a)) = \tau(a \cdot \tau(a) \cdot \tau^2(a) \cdots \tau^{n-1}(a))) = a \cdot \tau(a) \cdot \tau^2(a) \cdots \tau^{n-1}(a)) = N(a).$$

   Since τ generates G, $a \in \mathrm{Fix}(\langle \tau \rangle) = \mathrm{Fix}(G)$. Since $\mathrm{Fix}(G) = F$ by (11.2.6), $a \in F$.

3. Suppose $a = b/\tau(b)$ for some $b \in L$. Show that $N(a) = 1$.

   Sol. Since $\tau^n = 1$,

   $$N(a) = a\tau(a)\cdots\tau^{n-1}(a) = \frac{b}{\tau(b)}\frac{\tau(b)}{\tau^2(b)}\cdots\frac{\tau^{n-1}(b)}{\tau^n(b)} = 1.$$

4. Let $a \in L$ and $N(a) = 1$. By 1, there is an element $c \in L$ such that

   $$b = a\tau^0(c) + a\tau(a)\tau^1(c) + \cdots + (a\tau(a)\cdots\tau^{n-1}(a))\tau^{n-1}(c) \neq 0.$$

   Show that $a = b/\tau(b)$.

   Sol. It suffices to prove that $\tau(b) = b/a$.

   $$\begin{aligned} \tau(b) &= \tau(a)\tau(c) + \tau(a)\tau^2(a)\tau^2(c) + \cdots + (\tau(a)\tau^2(a)\cdots\tau^{n-1}(a)a)c \\ &= \frac{1}{a}(a\tau(a)\tau(c) + a\tau(a)\tau^2(a)\tau^2(c) + \cdots + (a\tau(a)\cdots\tau^{n-1}(a))\tau^{n-1}(c) + ac) = \frac{b}{a}. \end{aligned}$$

5. Suppose n is a prime and F contains a primitive n-th root of unity. Show that there is $a \in L$ such that $a^n \in F$ and $L = F(a)$.

   Sol. Let ζ be the primitive root of unity. Then $N(\zeta) = \zeta^n = 1$. Hence there is an element $b \in L$ such that $\zeta = b/\tau(b)$. Hence $b^n = \tau(b^n) \in F$ and $t^n - b^n \in F[t]$. Since $\zeta \neq 1$, $b \notin F$ and $L = F(b)$ as $(L : F) = n$ is prime.

Using this result one can show by induction that if $\mathrm{Gal}(f)$ *is solvable, then* f *is solvable by radicals.*