Final Exam solutions

Math 116: Finashin, Pamuk, Pierce, Solak

June 7, 2011, 13:30–15:30 (120 minutes)

Instructions. Work carefully. Your methods should be clear to the reader.

Problem 1 (12 points). *Is* $x^3 + x + 1$ *reducible over:*

(a) $\mathbb{Q}$ *?*

(b) $\mathbb{Z}_3$ *?*

(c) $\mathbb{Z}_5$ *?*

Solution. Since the polynomial (call it f) has degree 3, it is reducible if and only if it has a root.

(a) If p/q is a root, then p and q divide 1, so $p/q = \pm 1$. But $f(1) = 3$ and $f(-1) = -1$, so f has no roots and is irreducible over $\mathbb{Q}$.

(b) $f(1) = 0$, so f is reducible over $\mathbb{Z}_3$ (divisible by $(x-1)$).

(c) $f(0) = 1$, $f(1) = 3$, $f(2) = 11$, $f(3) = 31$, $f(4) = 69$; so f is irreducible over $\mathbb{Z}_5$.

Problem 2 (8 points). *Letting* $f(x) = 3x^4 + 5x^3 + x^2 + 5x - 2$, *write* $f(x)$ *as a product of irreducible polynomials over* $\mathbb{Q}$.

Solution. If p/q is a root of f, then $p \mid 2$ and $q \mid 3$, so $p \in \{\pm 1, \pm 2\}$ and $q \in \{\pm 1, \pm 3\}$, hence $p/q \in \{\pm 1, \pm 2, \pm\frac{1}{3}, \pm\frac{2}{3}\}$.

$$\begin{aligned} f(1) &= 3 + 5 + 1 + 5 - 2 \neq 0, \\ f(-1) &= 3 - 5 + 1 - 5 - 2 \neq 0, \\ f(2) &= 48 + 40 + 4 + 10 - 2 \neq 0, \\ f(-2) &= 48 - 40 + 4 - 10 - 2 = 0. \end{aligned}$$

Since -2 is a root, $f(x)$ is divisible by $(x+2)$. Using the division algorithm,

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

Also $1/3$ is a root of $3x^3 - x^2 + 3x - 1$, and

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

Therefore $\boxed{f(x) = (x+2)(3x-1)(x^2+1)}$. Since $(x+2)$ and $(3x-1)$ have degree 1, they are irreducible. Since $x^2+1 > 0$ for all x in $\mathbb{Q}$, it has no rational roots and is therefore irreducible.

Problem 3 (5 points)**.** *Is every integral domain a field? Explain.*

Solution. No, consider the ring of integers $(\mathbb{Z}, +, \cdot)$ which is an integral domain, since it has no zero divisors. But it is not a field, since the non-zero elements except ± 1 do not have multiplicative inverses.

Problem 4 (15 points)**.** *Find a polynomial $f(x)$ of least positive degree with the given properties. (Your answer should show the coefficients of $f(x)$.)*

(a) $f(x)$ is over $\mathbb{C}$, and $f(2\mathrm{i}) = 0 = f(1+\mathrm{i})$.

(b) $f(x)$ is over $\mathbb{R}$, and $2\mathrm{i}$ and $1+\mathrm{i}$ are zeros of it.

(c) $f(x)$ is over $\mathbb{Z}_2$, and 1 (that is, [1]) is a zero of multiplicity 4.

Answers.

(a) $f(x) = (x-2\mathrm{i})(x-1-\mathrm{i}) = x^2 - (1+3\mathrm{i})x + 2\mathrm{i} - 2$ over $\mathbb{C}$.

(b) $f(x) = (x-2\mathrm{i})(x+2\mathrm{i})(x-1-\mathrm{i})(x-1+\mathrm{i}) = (x^2+4)(x^2-2x+2) = x^4 - 2x^3 + 6x^2 - 8x + 8$ over $\mathbb{R}$.

(c) $f(x) = (x-1)^4 = x^4 - 4x^3 + 6x^2 - 4x + 1 = x^4 + 1$ over $\mathbb{Z}_2$.

Problem 5 (5 points)**.** *Over a field K, suppose $f(x)$ is a polynomial with no zeros in K. Must $f(x)$ be irreducible over K? Explain.*

Solution. No. For example, the polynomial $x^4 + 2x^2 + 1$ over $\mathbb{R}$ has no zeros in $\mathbb{R}$ but it is reducible over $\mathbb{R}$.

Problem 6 (15 points)**.** *Working over* $\mathbb{Z}_3$*, letting*

$$f(x) = x^5 + x + 1, \qquad\qquad g(x) = x^2 + 1,$$

find $s(x)$ *and* $t(x)$ *such that* $f(x) \cdot s(x) + g(x) \cdot t(x) = 1$.

Solution.

$$\begin{aligned} f(x) = x^5 + x + 1 &= g(x) \cdot (x^2 + 2x) + 2x + 1 \\ g(x) = x^2 + 1 &= (2x + 1) \cdot (2x + 2) + 2. \end{aligned}$$

Then

$$\begin{aligned} 2 &= g(x) - (2x + 1)(2x + 2) \\ &= g(x) - [f(x) - g(x)(x^3 + 2x)](2x + 2) \\ &= f(x)(x + 1) + g(x)[1 + (x^3 + 2x)(2x + 2)] \\ &= f(x)(x + 1) + g(x)(2x^4 + 2x^3 + x^2 + x + 1) \end{aligned}$$

Hence,

$$1 = f(x)(2x + 2) + g(x)(x^4 + x^3 + 2x^2 + 2x + 2).$$

So,

$$s(x) = 2x + 2, \qquad\qquad t(x) = x^4 + x^3 + 2x^2 + 2x + 2.$$

Problem 7 (20 points)**.** *Let* R *be the subring* $\{x + y\mathrm{i} \colon x, y \in \mathbb{Z}\}$ *of* $\mathbb{C}$*, and let* I *be the ideal* $\{x + y\mathrm{i} \colon x, y \in 2\mathbb{Z}\}$ *of* R*.*

(a) *How many additive cosets has* I *in* R*? List them clearly.*

(b) *Is the quotient* R/I *cyclic as an additive group? Explain.*

(c) *Show that the function* ϕ *from* R *to* $\mathbb{Z}_2$ *given by*

$$\phi(x + y\mathrm{i}) = [x + y] \qquad (*)$$

is a ring homomorphism.

(d) *Does the same formula* $(*)$ *define a ring homomorphism from* R *to* $\mathbb{Z}_3$*? Explain.*

Solution.

(a) Four cosets: I, $1 + I$, $\mathrm{i} + I$, and $1 + \mathrm{i} + I$.

(b) No: R/I has order 4, but each element has order 1 or 2.

(c)
$$\begin{aligned}\phi((a+b\mathrm{i})+(x+y\mathrm{i})) &= \phi(a+x+(b+y)\mathrm{i}) \\ &= [a+x+b+y] \\ &= [a+b]+[x+y] \\ &= \phi(a+b\mathrm{i})+\phi(x+y\mathrm{i}),\end{aligned}$$

$$\begin{aligned}\phi((a+b\mathrm{i})\cdot(x+y\mathrm{i})) &= \phi(ax-by+(ay+bx)\mathrm{i}) \\ &= [ax-by+ay+bx] \\ &= [ax+by+ay+bx] \\ &= [a+b]\cdot[x+y] \\ &= \phi(a+b\mathrm{i})\cdot\phi(x+y\mathrm{i}).\end{aligned}$$

(d) No, since $\phi(\mathrm{i}^2)=\phi(-1)=[-1]=[2]$, while $\phi(\mathrm{i})^2=[1]^2=[1]$.

Remark. For part (d), many people observed that the computations of (c) for multiplication were not justified *modulo* 3. This is correct, but one must show that the system of equations *fails* in at least one case. (In fact the system is correct when $3 \mid by$, but fails in all other cases.)