Solutions to Midterm Exam 1

Math 401

1. (10 points)

(a) Let $f = x^6 - 1$ and $g = x^4 - 1$ in $\mathbb{Q}[x]$. Calculate $d = \gcd(f, g)$. Find polynomials $a, b \in \mathbb{Q}[x]$ such that $af + bg = d$.

Solution: We run the Euclidean algorithm. Divide f by g to get a quotient x^2 and a remainder $x^2 - 1$:

$$f = x^2 \cdot g + (x^2 - 1).$$

Then we see that $x^2 - 1$ divides g evenly,

$$g = (x^2 - 1)(x^2 + 1),$$

so we stop. The conclusion is

$$d \;=\; x^2 - 1 \;=\; 1 \cdot f - x^2 \cdot g.$$

(b) List all *complex* roots of f and g. What roots do they have in common? Does this agree with the gcd you found above?

Solution: The six roots of f are ± 1 and $\frac{\pm 1 \pm \sqrt{3} i}{2}$, where the plus-or-minusses are taken independently. The four roots of g are ± 1 and $\pm i$. Thus f and g have two roots in common, 1 and -1, which are the two roots of $\gcd(f, g) = x^2 - 1$.

2. (20 points)

(a) Show that $f = 8x^3 - 6x - 1$ is irreducible in $\mathbb{Z}[x]$. Hint: Either show that it has no root in $\mathbb{Q}$ using the rational root test, or reduce mod 5 and show that it has no root in $\mathbb{Z}_5$. Why is this enough?

Solution: By Gauss's lemma, f is irreducible in $\mathbb{Z}[x]$ if and only if it is irreducible in $\mathbb{Q}[x]$. Because f is a cubic, it is reducible in $\mathbb{Q}[x]$ if and only if it has a root in $\mathbb{Q}$.

The rational root test says that if f has a root in $\mathbb{Q}$ then it has one of the from $\frac{r}{s}$, where $r \mid 1$ and $s \mid 8$. But we calculate:

$$\begin{array}{llll} f(1) = 1 & f(\frac{1}{2}) = -3 & f(\frac{1}{4}) = -\frac{19}{8} & f(\frac{1}{8}) = -\frac{111}{64} \\ f(-1) = -3 & f(-\frac{1}{2}) = 1 & f(-\frac{1}{4}) = \frac{3}{8} & f(-\frac{1}{8}) = -\frac{17}{64}. \end{array}$$

Thus f is irreducible.

Alternatively, if we reduce mod 5 we get $\bar{f} = 3x^3 + 4x + 4 \in \mathbb{Z}_5[x]$, which has no roots in $\mathbb{Z}_5$:

$$\bar{f}(0) = 4 \qquad \bar{f}(1) = 1 \qquad \bar{f}(2) = 1 \qquad \bar{f}(3) = 2 \qquad \bar{f}(4) = 2.$$

Thus $\bar{f}$ is irreducible in $\mathbb{Z}_5[x]$, so f is irreducible in $\mathbb{Z}[x]$.

(b) Calculate $f(-\frac{1}{2})$ and $f(\frac{1}{2})$. Conclude that f has three real roots.

Solution: Above we saw that $f(-\frac{1}{2}) = 1$ and $f(\frac{1}{2}) = -3$. Since the leading coefficient of f is positive, we know that $f(x) \to -\infty$ as $x \to -\infty$ and $f(x) \to +\infty$ as $x \to +\infty$. Thus f changes sign at least three times, so it has at least three real roots by the intermediate value theorem.

(c) Find the three real roots of f. You may use Cardano's formula: The roots of $z^3 + pz + q = 0$ are given by $v - \frac{p}{3v}$, where

$$v = \sqrt[3]{-\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}},$$

here you take one of the two square roots, but all three cube roots.

Solution: We divide through by 8 to get $x^3 - \frac{3}{4}x - \frac{1}{8}$, so we take $p = -\frac{3}{4}$ and $q = -\frac{1}{8}$. This gives

$$-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} = \frac{-1 + \sqrt{3}i}{16} = \frac{1}{8}e^{i\pi/3}.$$

Letting $\zeta = e^{i\pi/9} = \cos 20° + i \sin 20°$ we get

$$v = \begin{cases} \frac{1}{2}\zeta \\ \frac{1}{2}\zeta \cdot e^{2\pi i/3} = \frac{1}{2}\zeta^7 \\ \frac{1}{2}\zeta \cdot e^{4\pi i/3} = \frac{1}{2}\zeta^{13}. \end{cases}$$

Thus

$$x = v + \frac{1}{4v} = \begin{cases} \frac{1}{2}(\zeta + \zeta^{-1}) \\ \frac{1}{2}(\zeta^7 + \zeta^{-7}) \\ \frac{1}{2}(\zeta^{13} + \zeta^{-13}). \end{cases}$$

But $|z| = 1$, so $\zeta^{-1} = \bar{\zeta}$, so $\frac{1}{2}(\zeta^n + \zeta^{-n}) = \mathrm{Re}(\zeta^n) = \cos(n \cdot 20°)$ for all n, and thus

$$x = \begin{cases} \cos 20° \\ \cos 140° \\ \cos 260° = \cos 100°. \end{cases}$$

3. (25 points) Let R be an integral domain. Recall that an element $a \in R$ is called *irreducible* if it is not zero, not a unit, and $a = bc$ implies that b is a unit or c is a unit; and that a is called *prime* if $a \mid bc$ implies $a \mid b$ or $a \mid c$. In lecture we saw that if $a \neq 0$ and a is prime then a is irreducible. Here we will show the converse under some hypotheses.

(a) Let $a, b \in R$. Show that $a \mid b$ if and only if $(b) \subset (a)$.

Solution: If $(b) \subset (a)$ then $b \in (a)$, so $b = ax$ for some $x \in R$, so $a \mid b$. Conversely, if $a \mid b$ then we can write $b = ax$; now an arbitrary element of (b) is $by = axy \in (a)$.

(b) Let $a, b \in R$. Show that $a \mid b$ if and only if $(a, b) = (a)$.

Solution: Clearly we have $(b) \subset (a, b)$, so if $(a, b) = (a)$ then $(b) \subset (a)$, so $a \mid b$ by the previous part. For the converse, clearly we have $(a) \subset (a, b)$, so it is enough to show that if $a \mid b$ then $(a, b) \subset (a)$. Indeed, if $b = ax$ then an arbitrary element of (a, b) is

$$ay + bz = ay + axz = a(y + xz) \in (a),$$

as desired.

(c) Show that $a \in R$ is a unit if and only if $(a) = R$.

Solution: Observe that a is a unit if and only if $a \mid 1$, and that $(1) = R$. Thus by the first part, a is a unit if and only if $R \subset (a)$. But clearly $(a) \subset R$, so a is a unit if and only if $(a) = R$.

Now suppose that R is a *principal ideal domain*, that is, an integral domain where every ideal is generated by one element; in particular, for every $a, b \in R$ there is a $c \in R$ such that $(a, b) = (c)$.

(d) Show that if $a \in R$ is irreducible then for every $b \in R$, either $(a, b) = (a)$ or $(a, b) = R$.

Solution: Since R is a principal ideal domain, choose a $c \in R$ such that $(a, b) = (c)$. Then $a \in (c)$, so $a = cd$ for some $d \in R$, so either c is a unit or d is a unit. If c is a unit then $(c) = R$ by part c. If d is a unit then $(c) = (a)$, as we saw in homework.

(e) Show that if $a \in R$ is irreducible then a is prime. Hint: Suppose that $a \mid bc$ and $a \nmid b$; first argue that you can write $1 = ax + by$; then multiply through by c.

Solution: Following the hint, we suppose that $a \mid bc$ and $a \nmid b$; we want to show that $a \mid c$. By part b we have $(a, b) \neq (a)$, so by part d we have $(a, b) = R$, so $1 \in (a, b)$, so there are $x, y \in R$ such that $ax + by = 1$. Multiplying through by c we get $acx + bcy = c$. Since $a \mid bc$ we can write $bc = ad$ for some $d \in R$. Then

$$c = acx + bcy = acx + ady = a(cx + dy),$$

so $a \mid c$ as desired.