Math 461 **Exam 3**
Spring 2023 **Thurs Apr 27**

No electronic devices are allowed. There are 5 pages and each page is worth 6 points, for a total of 30 points.

Problem 1. Rational Root Test.

(a) Consider a rational polynomial $f(x) \in \mathbb{Q}[x]$ of degree 3. If $f(x)$ is not prime over $\mathbb{Q}$, prove that $f(x)$ has a root in $\mathbb{Q}$. [Hint: If $f(x)$ is not prime then we can write $f(x) = g(x)h(x)$ for some nonconstant polynomials $g(x), h(x) \in \mathbb{Q}[x]$.]

If $f(x)$ is not prime over $\mathbb{Q}$ then we can write $f(x) = g(x)h(x)$ for some nonconstant polynomials $g(x), h(x) \in \mathbb{Q}[x]$. Comparing degrees gives

$$3 = \deg(f) = \deg(g) + \deg(h).$$

Since $\deg(g), \deg(h) \geq 1$, one of these polynomials has degree 1. Without loss of generality suppose that $\deg(g) = 1$, so $g(x) = ax + b$ for some $a, b \in \mathbb{Q}$ with $a \neq 0$. But then we have

$$f(-b/a) = g(-b/a)h(-b/a) = 0h(-b/a) = 0,$$

hence $f(x)$ has a root $-b/a \in \mathbb{Q}$.

(b) Use the contrapositive of (a) and the rational root test to prove that the polynomial $x^3 - 2$ is prime over $\mathbb{Q}$.

The polynomial $x^3 - 2 \in \mathbb{Q}[x]$ has degree 3. If we can show that $x^3 - 2$ has no root in $\mathbb{Q}$ then it will follow from (a) that $x^3 - 2$ is prime over $\mathbb{Q}$.

Suppose for contradiction that $x^3 - 2$ does have a rational root $\alpha \in \mathbb{Q}$. We can write $\alpha = a/b$ for some $a, b \in \mathbb{Z}$ with $\gcd(a, b) = 1$. Then substituting gives

$$\begin{aligned} \alpha^3 - 2 &= 0 \\ (a/b)^3 - 2 &= 0 \\ a^3 - 2b^3 &= 0 \\ a^3 &= 2b^3. \end{aligned}$$

Since $a|2b^3$ and $\gcd(a, b) = 1$ we must have $a|2$. Similarly, since $b|a^3$ and $\gcd(a, b) = 1$ we must have $b|1$. We conclude that $\alpha = a/b = \pm 1, \pm 2$. But $(\pm 1)^3 - 2 \neq 0$ and $(\pm 2)^2 - 2 \neq 0$. Hence the polynomial $x^3 - 2$ has no rational root.

Problem 2. The Minimal Polynomial. Let $\mathbb{F}$ be a field and let $p(x) \in \mathbb{F}[x]$ be a prime polynomial. Let γ be an element of some larger field satisfying $p(\gamma) = 0$.

(a) For any polynomial $f(x) \in \mathbb{F}[x]$, prove that $f(\gamma) = 0$ implies $f(x) = p(x)g(x)$ for some $g(x) \in \mathbb{F}[x]$. [Hint: Let $f(\gamma) = 0$ and assume for contradiction that $f(x)$ is not a multiple of $p(x)$. Since $p(x)$ is prime, this implies that $\gcd(p, f) = 1$.]

Consider any $f(x) \in \mathbb{F}[x]$ satisfying $f(\gamma) = 0$. To prove that $p(x)|f(x)$ we assume for contradiction that $p(x) \nmid f(x)$. Since $p(x)$ is a prime element of the Euclidean domain $\mathbb{F}[x]$, this implies that $\gcd(p, f) = 1$. Then from the Extended Euclidean

Algorithm we can find $p'(x), f'(x) \in \mathbb{F}[x]$ satisfying $p(x)p'(x) + f(x)f'(x) = 1$. Finally, we substitute $x = \gamma$ to obtain the desired contradiction:

$$\begin{aligned} p(x)p'(x) + f(x)f'(x) &= 1 \\ p(\gamma)p'(\gamma) + f(\gamma)f'(\gamma) &= 1 \\ 0p'(\gamma) + 0f'(\gamma) &= 1 \\ 0 &= 1. \end{aligned}$$

(b) Let $\gamma = \sqrt[3]{2} \in \mathbb{R}$ be the real cube root of 2. For any rational polynomial $f(x) \in \mathbb{Q}[x]$, show that $f(\gamma) = 0$ implies $f(x) = (x^3 - 2)g(x)$ for some $g(x) \in \mathbb{Q}[x]$. [Hint: 1b.]

Consider the polynomial $p(x) = x^3 - 2 \in \mathbb{Q}[x]$. In Problem 1(b) we showed that $p(x)$ is a prime element of $\mathbb{Q}[x]$. Note that the real number $\gamma = \sqrt[3]{2}$ satisfies $p(\gamma) = 0$. Thus from part (a) we conclude for all rational polynomials $f(x) \in \mathbb{Q}[x]$ that

$$f(\gamma) = 0 \quad \Longrightarrow \quad f(x) = (x^3 - 2)g(x) \text{ for some } g(x) \in \mathbb{Q}[x].$$

Problem 3. Adjoining an Element to a Field. Let $\mathbb{F}$ be a field and let γ be an element of some larger field $\mathbb{E} \supseteq \mathbb{F}$. One can check that the set is a subring of $\mathbb{E}$:

$$\mathbb{F}[\gamma] = \{f(\gamma) : f(x) \in \mathbb{F}[x]\} \subseteq \mathbb{E}.$$

(a) Suppose that $p(\gamma) = 0$ for some polynomial $p(x) \in \mathbb{F}[x]$ of degree d. In this case show that every element of $\mathbb{F}[\gamma]$ can be expressed in the form $a_0 + a_1\gamma + \cdots + a_{d-1}\gamma^{d-1}$ for some $a_0, \ldots, a_{d-1} \in \mathbb{F}$. [Hint: A general element of $\mathbb{F}[\gamma]$ has the form $f(\gamma)$ for some $f(x) \in \mathbb{F}[x]$. Divide $f(x)$ by $p(x)$ to get a remainder.]

Let $p(x) \in \mathbb{F}[x]$ be any[1] polynomial of degree d satisfying $p(\gamma) = 0$ and consider any element $\alpha \in \mathbb{F}[\gamma]$. By definition we can write $\alpha = f(\gamma)$ for some polynomial $f(x) \in \mathbb{F}[x]$. Divide $f(x)$ by $p(x)$ to obtain polynomials $q(x), r(x) \in \mathbb{F}[x]$ satisfying

$$\begin{cases} f(x) = p(x)q(x) + r(x), \\ r(x) = 0 \text{ or } \deg(r) < d. \end{cases}$$

In either case we can write $r(x) = a_0 + a_1x + \cdots + a_{d-1}x^{d-1}$ for some numbers $a_0, a_1, \ldots, a_{d-1} \in \mathbb{F}$. Now substitute $x = \gamma$ to obtain

$$\begin{aligned} \alpha &= f(\gamma) \\ &= p(\gamma)q(\gamma) + r(\gamma) \\ &= 0q(\gamma) + r(\gamma) \\ &= r(\gamma) \\ &= a_0 + a_1\gamma + \cdots + a_{d-1}\gamma^{d-1}. \end{aligned}$$

(b) Again let $\gamma = \sqrt[3]{2} \in \mathbb{R}$. Express the number $1 + \gamma + \gamma^2 + \gamma^3 + \gamma^4 \in \mathbb{Q}[\gamma]$ in the standard form $a + b\gamma + c\gamma^2$ for some $a, b, c \in \mathbb{Q}$. [Hint: Divide $x^4 + x^3 + x^2 + x + 1$ by $x^3 - 2$ to get a remainder.]

Let $p(x) = x^3 - 2 \in \mathbb{Q}[x]$ and $f(x) = 1 + x + x^2 + x^3 + x^4 \in \mathbb{Q}[x]$. Divide $f(x)$ by $p(x)$ to obtain quotient $q(x) = x + 1$ and remainder $r(x) = x^3 + 3x + 3$:

[1] For this problem $p(x)$ need not be prime.

$$
\begin{array}{r l}
 & \phantom{x^4 + x^3 + x^2 +{}} x + 1 \\
x^3 - 2 \big) & x^4 + x^3 + x^2 \quad + x + 1 \\
 & - x^4 \qquad\qquad + 2x \\
\hline
 & \quad x^3 + x^2 + 3x + 1 \\
 & \quad - x^3 \qquad\quad + 2 \\
\hline
 & \qquad x^2 + 3x + 3
\end{array}
$$

It follows from part (a) that

$$1 + \gamma + \gamma^2 + \gamma^3 + \gamma^4 = f(\gamma) = r(\gamma) = 3 + 3\gamma + \gamma^2.$$

Alternatively, we can use the fact that $\gamma^3 = 2$ to obtain

$$\begin{aligned} 1 + \gamma + \gamma^2 + \gamma^3 + \gamma^4 &= 1 + \gamma + \gamma^2 + 2 + 2\gamma \\ &= 3 + 3\gamma + \gamma^2. \end{aligned}$$

Problem 4. Existence of Inverses. Let $p(x) \in \mathbb{F}[x]$ be **prime** over a field $\mathbb{F}$ and let $p(\gamma) = 0$ for a number γ in some larger field.

(a) Consider a polynomial $f(x) \in \mathbb{F}[x]$ such that $f(\gamma) \neq 0$. In this case show that $f(x)$ is not a multiple of $p(x)$ in the ring $\mathbb{F}[x]$.

Consider any polynomial $f(x) \in \mathbb{F}[x]$ such that $f(\gamma) \neq 0$. If we had $f(x) = p(x)g(x)$ for some $g(x) \in \mathbb{F}[x]$ then we would obtain a contradiction:

$$f(\gamma) = p(\gamma)g(\gamma) = 0g(\gamma) = 0.$$

Hence $f(x)$ is not a multiple of $p(x)$.

(b) Prove that the ring $\mathbb{F}[\gamma]$ from Problem 3 is actually a field. [Hint: An arbitrary element of $\mathbb{F}[\gamma]$ has the form $f(\gamma)$ for some polynomial $f(x)$. If $f(\gamma) \neq 0$, use part (a) to show that $\gcd(p, f) = 1$ in the ring $\mathbb{F}[x]$.]

Consider an arbitrary nonzero element $\alpha \in \mathbb{F}[\gamma]$. By definition we can write $\alpha = f(\gamma)$ for some (nonzero) polynomial $f(x) \in \mathbb{F}[x]$. Since $f(\gamma) = \alpha \neq 0$ part (a) tells us that $f(x)$ is not a multiple of $p(x)$. Since $p(x)$ is a prime element of the Euclidean domain $\mathbb{F}[x]$ this implies that $\gcd(p, f)$, hence we can find polynomials $p'(x), f'(x) \in \mathbb{F}[x]$ satisfying $p(x)p'(x) + f(x)f'(x) = 1$. Substitute $x = \gamma$ to obtain

$$\begin{aligned} p(x)p'(x) + f(x)f'(x) &= 1 \\ p(\gamma)p'(\gamma) + f(\gamma)f'(\gamma) &= 1 \\ 0p'(\gamma) + f(\gamma)f'(\gamma) &= 1 \\ f(\gamma)f'(\gamma) &= 1 \\ \alpha f'(\gamma) &= 1. \end{aligned}$$

Thus $f'(\gamma) \in \mathbb{F}[\gamma]$ is a multiplicative inverse of α.

Problem 5. Example. Let $\gamma = \sqrt[3]{2} \in \mathbb{R}$. From the previous problems we know that the following set is a subfield of $\mathbb{R}$:

$$\mathbb{Q}[\gamma] = \{a + b\gamma + c\gamma^2 : a, b, c \in \mathbb{Q}\}.$$

(a) Express the product $(1+\gamma^2)(1-\gamma^2)$ in standard form $a+b\gamma+c\gamma^2$.

Since $\gamma^3 = 2$ we have $(1+\gamma^2)(1-\gamma^2) = 1-\gamma^4 = 1-2\gamma+0\gamma^2$.

Remark: This is not a good problem. (I was a bit rushed when I wrote the exam.)

(b) Express the inverse $(1+\gamma^2)^{-1}$ in standard form $a+b\gamma+c\gamma^2$. [Hint: Expand the left side of $(1+\gamma^2)(a+b\gamma+c\gamma^2) = 1+0\gamma+0\gamma^2$ and compare coefficients.]

There are two ways to do this. The proof of Problem 4(b) suggests using the Extended Euclidean Algorithm in the ring $\mathbb{Q}[x]$. I don't suggest this method because it's too easy to make mistakes, but here it is. Consider all triples of polynomials $f(x), g(x), h(x)$ satisfying $(x^3-2)f(x) + (x^2+1)g(x) = h(x)$. Begin with the easy triples $(f,g,h) = (1, 0, x^3-2)$ and $(f,g,h) = (0, 1, x^2+1)$, then perform row operations to obtain a triple of the form $(f, g, 1)$:

$f(x)$	$g(x)$	$h(x)$
1	0	x^3-2
0	1	x^2+1
1	$-x$	$-x-2$
$x-2$	$-x^2+2x+1$	5
$\frac{x-2}{5}$	$\frac{-x^2+2x+1}{5}$	1

We conclude that

$$(1+\gamma^2)^{-1} = \frac{-\gamma^2+2\gamma+1}{5} = -\frac{1}{5}\gamma^2 + \frac{2}{5}\gamma + \frac{1}{5}.$$

It is easier to use linear algebra over $\mathbb{Q}$. Let $(1+\gamma^2)^{-1} = a+b\gamma+c\gamma^2$, so that $(1+\gamma^2)(a+b\gamma+c\gamma^2) = 1+0\gamma+0\gamma^2$. Expand the left side to get

$$\begin{aligned}
(1+\gamma^2)(a+b\gamma+c\gamma^2) &= 1+0\gamma+0\gamma^2 \\
a+b\gamma+c\gamma^2+a\gamma^2+b\gamma^3+c\gamma^4 &= 1+0\gamma+0\gamma^2 \\
a+b\gamma+c\gamma^2+a\gamma^2+b2+c2\gamma &= 1+0\gamma+0\gamma^2 \\
(a+2b)+(b+2c)\gamma+(a+c)\gamma^2 &= 1+0\gamma+0\gamma^2.
\end{aligned}$$

Then compare coefficients[2] to get the system

$$\begin{cases} a + 2b + 0 = 1, \\ 0 + b + 2c = 0, \\ a + 0 + c = 0, \end{cases}$$

which has solution $a = 1/5$, $b = 2/5$ and $c = -1/5$. Hence

$$(1+\gamma^2)^{-1} = a+b\gamma+c\gamma^2 = \frac{1}{5} + \frac{2}{5}\gamma - \frac{1}{5}\gamma^2.$$

[2]Here we are using the fact that $a+b\gamma+c\gamma^2 = d+e\gamma+f\gamma^2$ implies $(a,b,c) = (d,e,f)$ for $a,b,c,d,e,f \in \mathbb{Q}$, which we did not prove on this exam. It follows from the fact that x^2-3 is prime over $\mathbb{Q}[x]$.