ABSTRACT ALGEBRA II MIDTERM REVIEW

MARIO L. GUTIERREZ ABED

Problem 1. (7 pts each)

a) Show that $\mathbb{Z}_2[x]/\langle x^3+1\rangle$ is not a field. (State theorem(s) involved)

Solution. Notice that x^3+1 is reducible because $x^3+1=(x+1)(x^2-x+1)$ (this follows from the algebraic identity $a^3+b^3=(a+b)(a^2-ab+b^2)$). But then we know from a previous theorem that a nontrivial ideal $\langle p(x)\rangle \in F[x]$ is maximal iff $p(x)$ is irreducible over F. Hence, since in this case $p(x)=x^3+1$ is reducible, we have that $\langle p(x)\rangle$ is not maximal in $F[x]$, and by another theorem that says that $\mathcal{R}/\mathcal{I}$ is a field if and only if $\mathcal{I}$ is a maximal ideal, we have the desired result that $\mathbb{Z}_2[x]/\langle x^3+1\rangle$ is not a field. $\square$

b) Give an example of a ring $\mathcal{R}$ in which a cubic polynomial from $\mathcal{R}[x]$ can be written as a product of two quadratic polynomials from $\mathcal{R}[x]$.

Solution. Take $\mathcal{R}=\mathbb{Z}_4$ and consider the product of two quadratic polynomials:

$$\begin{aligned}(2x^2+x)(2x^2+1) &= 2x^2(2x^2+1)+x(2x^2+1)\\ &= \underbrace{4x^2}_{=0 \text{ in } \mathbb{Z}_4} +2x^2+2x^3+x\\ &= 2x^3+2x^2+x.\end{aligned}$$

Hence this product of two quadratic polynomials in $\mathbb{Z}_4$ yields a cubic polynomial in $\mathbb{Z}_4$, as desired. $\square$

c) Show that $f(x)=x^5-6x^4+15x^3+21x^2+15x+6$ is irreducible over $\mathbb{Q}$. (State theorem(s) involved)

Solution. According to the *Einstenstein's Criterion*, if we let $f(x)=a_0+\cdots+a_nx^n$ be a polynomial in $\mathbb{Z}[x]$ and suppose there exists a prime p such that the following three properties hold:

- $p \nmid a_n$
- $p \mid a_{n-1},\ldots,a_0$

- $p^2 \nmid a_0$,

then we have that $f(x)$ is irreducible over $\mathbb{Q}[x]$.

Now notice that in our particular example $f(x) = x^5 - 6x^4 + 15x^3 + 21x^2 + 15x + 6$ is irreducible over $\mathbb{Q}$ for $p = 3$, since

- $3 \nmid 1$
- $3 \mid -6, 15, 21, 15, 6$
- $3^2 = 9 \nmid 6$. □

d) Let α be a zero of $x^3 + x + 1$ in some extension field of $\mathbb{Z}_2$. Show that $\alpha + 1$ is a zero of $x^3 + x^2 + 1$.

Solution. Since α is a zero of $x^3 + x + 1$ in some extension field of $\mathbb{Z}_2$, then

$$\begin{aligned} &\alpha^3 + \alpha + 1 = 0 \\ \implies &\alpha^3 = -\alpha - 1 \\ &\quad\;\, = \alpha + 1 \quad \text{in } \mathbb{Z}_2. \end{aligned}$$

Then we have

$$\begin{aligned} x^3 + x^2 + 1 \,|_{x=\alpha+1} &= (\alpha+1)^3 + (\alpha+1)^2 + 1 \\ &= (\alpha+1)(\alpha+1)^2 + (\alpha+1)^2 + 1 \\ &= \alpha^3(\alpha+1)^2 + (\alpha+1)^2 + 1 \\ &= \alpha^3(\alpha^2 + 2\alpha + 1) + \alpha^2 + 2\alpha + 1 + 1 \\ &= \alpha^5 + \underbrace{2\alpha^4}_{=0} + \alpha^3 + \alpha^2 + \underbrace{2\alpha}_{=0} + \underbrace{2}_{=0} \\ &= \alpha^5 + \alpha^3 + \alpha^2 \\ &= \alpha^2(\alpha^3 + \alpha + 1) \\ &= \alpha^2(0) = 0. \end{aligned}$$

□

e) Show that $f(x) = x^2 + x + 3$ is reducible over $\mathbb{Z}_5$. (State theorem(s) involved)

Solution. Recall the theorem that says that if $f(x) \in F[x]$, where $f(x)$ is of degree 2 or 3, then $f(x)$ is reducible over F if and only if it has a zero in F. Now notice that 1 is a zero for $f(x) = x^2 + x + 3$, since $f(1) = 1^2 + 1 + 3 = 0$ in $\mathbb{Z}_5[x]$. Hence we have shown that $f(x) = x^2 + x + 3$ is reducible over $\mathbb{Z}_5$, as desired.

Notice that $f(x)$ reduces to $(x-1)(x-3)$ because

$$\begin{aligned} x^2+1x+3 &= x^2-4x+3 \qquad (\text{Since } 1=-4 \text{ in } \mathbb{Z}_5) \\ &= (x-1)(x-3). \end{aligned}$$

□

Problem 2. (5 pts each) In each part give an example (with a brief explanation) that satisfies the given conditions or briefly explain why no such example exists.

a) $\mathcal{R}$ and $\mathcal{S}$ are fields. A polynomial $f(x)$ irreducible in $\mathcal{R}[x]$ but reducible in $\mathcal{S}$.

Solution. Take $\mathcal{R}=\mathbb{R}$ and $\mathcal{S}=\mathbb{C}$, and consider the polynomial $f(x)=x^2+1$ in $\mathbb{R}[x]$, which is irreducible over $\mathbb{R}$ because $f(x)$ has no zero in $\mathbb{R}$ (this fact is justified by the theorem invoked in *Exercise 1e)* above). However we have that $f(x)$ is reducible over $\mathcal{S}=\mathbb{C}$, because $f(x)=x^2+1=(x-i)(x+i)$ in $\mathbb{C}[x]$, which gives us zeroes $\pm i \in \mathbb{C}$. □

b) A factor ring $\mathcal{R}/\mathcal{I}$ that is a field, of a ring $\mathcal{R}$ that is an integral domain (but not necessarily a field).

Solution. Take $\mathcal{R}=\mathbb{Z}$, which is an integral domain, and take $\mathcal{I}=2\mathbb{Z}$. Then we have the factor ring $\mathcal{R}/\mathcal{I}=\mathbb{Z}/2\mathbb{Z}$, which is isomorphic to $\mathbb{Z}_2$, and hence is a field. (Alternatively, we could have made the observation that $2\mathbb{Z}$ is a maximal ideal and, since $\mathbb{Z}$ is a commutative ring with unity, we may conclude by a previous theorem that $\mathbb{Z}/2\mathbb{Z}$ must be a field). □

c) A factor ring $\mathcal{R}/\mathcal{I}$ that is a field, of a ring $\mathcal{R}$ which is not an integral domain.

Solution. Take $\mathcal{R}=\mathbb{Z}_4$, which is not an integral domain (because it has the zero divisor 2: $2\neq 0$, but $2\cdot 2=0$) and take $\mathcal{I}=\{0,2\}$. Then we have the factor ring $\mathcal{R}/\mathcal{I}=\mathbb{Z}_4/\{0,2\}$, which is isomorphic to $\mathbb{Z}_2$, and hence is a field. (Again, we could have made the observation that $\{0,2\}$ is a maximal ideal and, since $\mathbb{Z}_4$ is a commutative ring with unity, we could conclude by a previous theorem that $\mathbb{Z}_4/\{0,2\}$ must be a field). □

d) A ring $\mathcal{R}$ containing no proper nontrivial ideals.

Solution. By a previous theorem we know that a field contains no proper nontrivial ideals. Hence, as an example, take the ring $\mathcal{R}=\mathbb{R}$, which is a field and consequently it has no proper nontrivial ideals. □

e) A maximal ideal $\mathcal{M}$ in a commutative ring $\mathcal{R}$ with unity that is not a prime ideal.

Solution. No such example exists. We have a theorem that says that every maximal ideal in a commutative ring with unity is a prime ideal. □

f) A polynomial $f(x) \in F[x]$ of degree 4 or more, containing no zeroes in F, but reducible in $F[x]$.

Solution. Let's go with a simple one. Take $f(x) = x^4 + 2x^2 + 1$ in $\mathbb{R}[x]$. This polynomial reduces to the product of two quadratic factors $(x^2+1)(x^2+1)$, which has zeroes $\pm i \notin \mathbb{R}$. □

Problem 3. (15 pts) Show that $f(x) = x^4 - 10x^2 + 1$ is irreducible in $\mathbb{Q}[x]$.

Solution. If $f(x) = x^4 - 10x^2 + 1$ were reducible in $\mathbb{Q}[x]$, then either it factors into quadratic terms or it has a linear factor. We will analyze both cases now and show that such factorization is impossible in either case:

• Case I : If $f(x)$ has a linear factor in $\mathbb{Q}[x]$, then it has a zero in $\mathbb{Q}$ by a previous theorem. But then by a previous corollary, we know that if $f(x) = a_0 + \cdots + a_{n-1}x^{n-1} + x^n$ is a polynomial with integral coefficients and with $a_0 \neq 0$, and if $f(x)$ has a zero in $\mathbb{Q}$, then it has a zero α in $\mathbb{Z}$, and α must divide a_0.

But then in our example $a_0 = 1$, hence we have that α must divide 1, i.e. $\alpha = \pm 1$. But

$$f(1) = 1^4 - 10(1)^4 + 1 = -8 \neq 0$$
$$f(-1) = (-1)^4 - 10(-1)^4 + 1 = -8 \neq 0,$$

so the factorization is impossible.

• Case II : By a previous theorem we have that if $f(x) \in \mathbb{Z}[x]$, then $f(x)$ factors into a product of polynomials of lower degrees r and s in $\mathbb{Q}[x]$ iff it has such a factorization with polynomials of the same degrees r and s in $\mathbb{Z}[x]$. Hence if $f(x)$ factors into quadratic factors in $\mathbb{Q}[x]$, we can write it in the form

$$x^4 - 10x^2 + 1 = (x^2 + ax + b)(x^2 + cx + d) \qquad \text{where } a, b, c, d \in \mathbb{Z}$$

Now expanding on the right hand side we get $x^4 + (c+a)x^3 + (d+ac+b)x^2 + (ad+bc)x + bd$, which gives us the linear system of equations

$$\begin{aligned} c + a &= 0 \\ d + ac + b &= -10 \\ ad + bc &= 0 \\ bd &= 1. \end{aligned}$$

It can be shown by a straight computation that such system of equations is inconsistent. Thus the factorization of $f(x)$ into quadratic factors in $\mathbb{Q}[x]$ is impossible, and the second case also fails.

Hence we have shown that $f(x) = x^4 - 10x^2 + 1$ is irreducible in $\mathbb{Q}[x]$, as desired. □

Problem 4. (20 pts)

a) Let $f(x) \in F[x]$, and let $f(x)$ be of degree 2 or 3. Prove that $f(x)$ is reducible over F if and only if it has a zero in F.

Proof. ($\Rightarrow$) Let $f(x)$ be reducible over F so that $f(x) = g(x)h(x)$, where both $\deg(g(x))$ and $\deg(h(x))$ are $< \deg(f(x))$. Then, since $f(x)$ is either quadratic or cubic, we must have that either $g(x)$ or $h(x)$ is of degree 1. Now, WLOG, take $\deg(g(x)) = 1$. Then except for a possible factor in F, $g(x)$ is of the form $x - \alpha$. Hence $g(\alpha) = 0$, which in turn implies that $f(\alpha) = 0 \cdot h(\alpha) = 0$, so $f(x)$ has a zero in F.

($\Leftarrow$) This direction is trivial, since by a previous corollary we already know that if $f(\alpha) = 0$ for $\alpha \in F$, then $x - \alpha$ is a factor of $f(x)$, thus $f(x)$ is indeed reducible over F. $\square$

b) If $\mathcal{R}$ is a ring with unity, and $\mathcal{I}$ is an ideal of $\mathcal{R}$ containing a unit, then $\mathcal{I} = \mathcal{R}$.

Proof. Let $\mathcal{I}$ be an ideal of $\mathcal{R}$, and suppose that $u \in \mathcal{I}$ for some unit u in $\mathcal{R}$. Then the condition

$$(\dagger) \qquad r\mathcal{I} \subseteq \mathcal{I} \quad \forall\, r \in \mathcal{R}$$

implies, if we take $r = u^{-1}$ and $u \in \mathcal{I}$, that $1 = u^{-1}u$ is in $\mathcal{I}$. But then ($\dagger$) implies that $r1 = r$ is in $\mathcal{I}$ for all $r \in \mathcal{R}$, so $\mathcal{I} = \mathcal{R}$. $\square$

c) Let $\mathcal{R}$ be a commutative ring with unity and let $\mathcal{I}$ be an ideal in $\mathcal{R}$. Then the quotient ring $\mathcal{R}/\mathcal{I}$ is a field if and only if $\mathcal{I}$ is a maximal ideal.

Proof. ($\Rightarrow$) Suppose that $\mathcal{R}/\mathcal{I}$ is a field. By a previous proposition we know that if $\mathcal{N}$ is any ideal of $\mathcal{R}$ such that $\mathcal{I} \subset \mathcal{N} \subset \mathcal{R}$ and $\gamma \colon \mathcal{R} \to \mathcal{R}/\mathcal{I}$ is the canonical homomorphism of $\mathcal{R}$ onto $\mathcal{R}/\mathcal{I}$, then $\gamma[\mathcal{N}]$ is an ideal of $\mathcal{R}/\mathcal{I}$ with

$$\{(0 + \mathcal{I})\} \subset \gamma[\mathcal{N}] \subset \mathcal{R}/\mathcal{I}.$$

But this is contrary to a previous corollary which says that a field does not contain any proper nontrivial ideals. Hence if $\mathcal{R}/\mathcal{I}$ is a field, then the ideal $\mathcal{I}$ is maximal.

($\Leftarrow$) Conversely, suppose $\mathcal{I}$ is maximal in $\mathcal{R}$. Observe that if $\mathcal{R}$ is a commutative ring with unity, then $\mathcal{R}/\mathcal{I}$ is also a nonzero commutative ring with unity if $\mathcal{I} \neq \mathcal{R}$, which is indeed the case if $\mathcal{I}$ is maximal.

Now let $(a + \mathcal{I}) \in \mathcal{R}/\mathcal{I}$, with $a \notin \mathcal{I}$, so that $a + \mathcal{I}$ is not the additive identity element in $\mathcal{R}/\mathcal{I}$. Suppose that $a + \mathcal{I}$ has no multiplicative inverse in $\mathcal{R}/\mathcal{I}$. Then the set

$$(\mathcal{R}/\mathcal{I})(a + \mathcal{I}) = \{(r + \mathcal{I})(a + \mathcal{I}) \mid (r + \mathcal{I}) \in \mathcal{R}/\mathcal{I}\}$$

does not contain $1+\mathcal{I}$. We can easily see that $(\mathcal{R}/\mathcal{I})(a+\mathcal{I})$ is an ideal of $\mathcal{R}/\mathcal{I}$, which is nontrivial because $a \notin \mathcal{I}$ and it is also proper because it does not contain $1+\mathcal{I}$.

Now consider the canonical homomorphism $\gamma\colon \mathcal{R} \to \mathcal{R}/\mathcal{I}$ and notice that $\gamma^{-1}[(\mathcal{R}/\mathcal{I})(a+\mathcal{I})]$ is a proper ideal of $\mathcal{R}$ properly containing $\mathcal{I}$. But this contradicts our assumption that $\mathcal{I}$ is maximal, so $a+\mathcal{I}$ must have a multiplicative inverse in $\mathcal{R}/\mathcal{I}$, and thus $\mathcal{R}/\mathcal{I}$ must be a field. □

d) Let $\mathcal{R}$ be a commutative ring with unity, and let $\mathcal{I} \neq \mathcal{R}$ be an ideal in $\mathcal{R}$. Then $\mathcal{R}/\mathcal{I}$ is an integral domain if and only if $\mathcal{I}$ is a prime ideal in $\mathcal{R}$.

Proof. This result is quite trivial. Let $\mathcal{R}/\mathcal{I}$ be an integral domain and notice that for any two elements $a+\mathcal{I}, b+\mathcal{I} \in \mathcal{R}/\mathcal{I}$, where $a, b \in \mathcal{R}$, we have

$$(a+\mathcal{I})(b+\mathcal{I}) = ab+\mathcal{I}.$$

Now notice that if $ab+\mathcal{I} = \mathcal{I}$, then we must have that either $a \in \mathcal{I}$ or $b \in \mathcal{I}$, since the coset $\mathcal{I}$ plays the role of 0 in $\mathcal{R}/\mathcal{I}$, and by the definition of an integral domain $\mathcal{R}/\mathcal{I}$ has no zero divisors. But looking at the coset representatives, we see that this condition amounts to saying that $ab \in \mathcal{I}$ implies that either $a \in \mathcal{I}$ or $b \in \mathcal{I}$, which is in fact the definition of a prime ideal. □

e) **(Kronecker's Theorem)** Let F be a field and let $f(x)$ be a non-constant polynomial in $F[x]$. Then there exists an extension field E of F and an $\alpha \in E$ such that $f(\alpha) = 0$.

Proof. By *Theorem 23.20*[1], $f(x)$ has a factorization in $F[x]$ into polynomials that are irreducible over F. Let $p(x)$ be an irreducible polynomial in such a factorization. It is clearly sufficient to find an extension field E of F containing an element α such that $p(\alpha) = 0$.

Take the maximal ideal $\langle p(x)\rangle$ in $F[x]$, so that $F[x]/\langle p(x)\rangle$ is a field (we know this from a previous theorem). We claim that F can be identified with a subfield of $F[x]/\langle p(x)\rangle$ in a natural way by use of the map $\psi\colon F \to F[x]/\langle p(x)\rangle$ given by

$$\psi(a) = a + \langle p(x)\rangle \qquad \text{for } \ a \in F.$$

[1]Here's *Theorem 23.20* for reference:
If F is a field, then every nonconstant polynomial $f(x) \in F[x]$ can be factored in $F[x]$ into a product of irreducible polynomials, the irreducible polynomials being unique expect for order and for unit (that is, nonzero constant) in F.

Notice that this map is injective:

$$\begin{aligned} &\psi(a) = \psi(b) \\ \implies &a + \langle p(x) \rangle = b + \langle p(x) \rangle \qquad \text{for some } a, b \in F \\ \implies &(a - b) \in \langle p(x) \rangle, \end{aligned}$$

so $a - b$ must be a multiple of the polynomial $p(x)$, which is of degree ≥ 1. Now $a, b \in F \implies a - b \in F$. Thus we must have $a - b = 0 \implies a = b$.

We defined addition and multiplication in $F[x]/\langle p(x) \rangle$ by choosing any representatives, so we may choose $a \in (a + \langle p(x) \rangle)$. Thus ψ is a homomorphism that maps F injectively onto a subfield of $F[x]/\langle p(x) \rangle$. We identify F with $\{a + \langle p(x) \rangle \mid a \in F\}$ by means of this map ψ. Thus we shall view $E = F[x]/\langle p(x) \rangle$ as an extension field of F. Hence we have manufactured our desired extension field E of F, and all that remains for us to show is that E contains a zero of $p(x)$:

Let us set

$$\alpha = x + \langle p(x) \rangle,$$

so $\alpha \in E$. Consider the evaluation homomorphism $\phi_\alpha \colon F[x] \to E$. If $p(x) = a_0 + a_1 x + \cdots + a_n x^n$, where $a_i \in F$, then we have

$$\phi_\alpha(p(x)) = a_0 + a_1(x + \langle p(x) \rangle) + \cdots + a_n(x + \langle p(x) \rangle)^n$$

in $E = F[x]/\langle p(x) \rangle$. But we can compute in $F[x]/\langle p(x) \rangle$ by choosing representatives, and x is a representative of the coset $\alpha = x + \langle p(x) \rangle$. Therefore,

$$\begin{aligned} p(\alpha) &= (a_0 + a_1 x + \cdots + a_n x^n) + \langle p(x) \rangle \\ &= p(x) + \langle p(x) \rangle = \langle p(x) \rangle = 0 \end{aligned}$$

in $F[x]/\langle p(x) \rangle$. We have thus found an element $\alpha \in E = F[x]/\langle p(x) \rangle$ such that $p(\alpha) = 0$, and therefore $f(\alpha) = 0$. $\square$

f) Let F be a field and $f(x) \neq 0$ be a polynomial in $F[x]$. Let α be a root of $f(x)$ in an extension field E of F. Then α is a multiple root of $f(x)$ if and only if $f'(\alpha) = 0$.

Proof. ($\Rightarrow$) Suppose α is a multiple root of $f(x)$, so that $(x - \alpha)^2$ divides $f(x)$, i.e. $f(x) = (x - \alpha)^2 g(x)$ for some $g(x) \in F[x]$. Then

$$\begin{aligned} f'(x) &= (x - \alpha)^2 g'(x) + g(x) \cdot 2(x - \alpha) \\ &= (x - \alpha)[(x - \alpha) g'(x) + 2g(x)] \\ \implies f'(\alpha) &= 0. \end{aligned}$$

($\Leftarrow$) Conversely, suppose we have $f'(\alpha) = 0$. Notice that if $\deg(f(x)) = 1$, then $f(x)$ is a linear polynomial of the form $b(x-\alpha)$, and so $f'(\alpha) = b$, which contradicts our hypothesis. Thus we only need to consider the case when $\deg(f(x)) \geq 2$.

By the division algorithm,
$$f(x) = (x-\alpha)^2 g(x) + r(x),$$
where $\deg(r(x)) = 0$ or $\deg(r(x)) < \deg((x-\alpha)^2) = 2$. In other words, we must have $\deg(r(x)) \leq 1$, which we consider as separate cases:

- Case I : Let $r(x)$ be a constant term b. Then
$$\begin{aligned} f(x) &= (x-\alpha)^2 g(x) + b \\ \Longrightarrow f'(x) &= (x-\alpha)^2 g'(x) + 2g(x)(x-\alpha) \\ \Longrightarrow f'(\alpha) &= 0. \end{aligned}$$

- Case II : Let $r(x)$ be a linear term $b(x-\alpha)$. Then
$$\begin{aligned} f(x) &= (x-\alpha)^2 g(x) + b(x-\alpha) \\ \Longrightarrow f'(x) &= (x-\alpha)^2 g'(x) + 2g(x)(x-\alpha) + b \\ \Longrightarrow f'(\alpha) &= b. \qquad (\Rightarrow\Leftarrow) \end{aligned}$$

Hence the case where $\deg(r(x)) = 1$ fails, and so we see that α cannot be a simple root when $f'(\alpha) = 0$. $\square$