ABSTRACT ALGEBRA II FINAL REVIEW

MARIO L. GUTIERREZ ABED

Problem 1. (5 pts each)

a) Decide whether i is in the field $E = \mathbb{Q}(\sqrt{-2})$.

Solution. Let $E = \mathbb{Q}(\sqrt{-2})$. If $i \in E$, then

$$\alpha = i\sqrt{-2} \in E.$$

But from this we get that

$$\begin{aligned} &\alpha^2 - 2 = 0 \\ \implies\ &\alpha = \pm\sqrt{2}. \end{aligned}$$

Then, since $E = \mathbb{Q}(\sqrt{-2}) = \{a + b\sqrt{-2} \mid a, b \in \mathbb{Q}\}$, we must have that $\alpha = \sqrt{2}$ is of the form

$$\sqrt{2} = a + b\sqrt{-2} \in E.$$

But then,

$$\begin{aligned} &(\sqrt{2})^2 = (a + b\sqrt{-2})^2 \\ \implies\ &2 = a^2 + 2ab\sqrt{-2} - 2b^2 \\ \implies\ &\frac{2 - a^2 + 2b^2}{2ab} = \sqrt{-2}. \end{aligned}$$

But this is not possible because $(2 - a^2 + 2b^2)/(2ab) \in \mathbb{Q}$ (since $a, b \in \mathbb{Q}$), while $\sqrt{-2} \notin \mathbb{Q}$. ($\Rightarrow\Leftarrow$).

Thus, we must have that $i \notin E$. $\square$

b) In $\mathbb{Z}_3[x]$, write $x^3 + 2$ as a product of linear factors.

Solution. We have

$$\begin{aligned} x^3 + 2 &= x^3 - 1 && \text{(Because } 2 = -1 \text{ in } \mathbb{Z}_3\text{)} \\ &= (x-1)(x^2 + x + 1) && \text{(By the identity } x^3 - a^3 = (x-a)(x^2 + xa + a^2)\text{)} \\ &= (x-1)(x-1)(x-1) \\ &= (x+2)(x+2)(x+2). \quad \square \end{aligned}$$

c) Show that $f(x) = 25x^5 - 9x^4 - 3x^2 - 12$ is irreducible over $\mathbb{Q}$. (State theorem(s) involved)

Solution. According to Eisenstein's criterion, if we let $f(x) = a_0 + \cdots + a_n x^n$ 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 in $\mathbb{Q}[x]$.

Now notice that in our particular example $f(x) = 25x^5 - 9x^4 - 3x^2 - 12$ is irreducible over $\mathbb{Q}$ for $p = 3$, since

- $3 \nmid 25$
- $3 \mid -9, -3, -12$
- $3^2 = 9 \nmid -12$. □

d) Find the minimal polynomial for $\sqrt{2} + i$ over $\mathbb{Q}$.

Solution. Let $\alpha = \sqrt{2} + i$. Then we have

$$\begin{aligned} \alpha^2 = (\sqrt{2}+i)^2 &= 2 + 2\sqrt{2}i - 1 \\ \implies \alpha^2 - 1 &= 2\sqrt{2}i \\ \implies (\alpha^2-1)^2 &= (2\sqrt{2}i)^2 \\ \implies \alpha^4 - 2\alpha^2 + 1 &= -8 \\ \implies \alpha^4 - 2\alpha^2 + 9 &= 0. \end{aligned}$$

Hence, the minimal polynomial for $\sqrt{2} + i$ over $\mathbb{Q}$ is $x^4 - 2x^2 + 9$. □

e) Does the polynomial $x^5 + x + 1$ have a multiple root in some extension field of $\mathbb{Z}_3$.

Solution. We use the following proposition:

> Let F be a field and let $f(x) \in F[x]$, with $f(x) \neq 0$. Let α be a zero of $f(x)$ in some extension field E of F. Then α is a multiple root of $f(x)$ in E if and only if $f'(\alpha) = 0$.

Since in this case we have

$$f(1) = 1^5 + 1 + 1 = 0 \in \mathbb{Z}_3$$

and

$$f'(1) = 5(1)^4 + 1 = 0 \in \mathbb{Z}_3,$$

we must have by the above proposition that the polynomial $f(x)$ does have a multiple root in some extension field of $\mathbb{Z}_3$. $\square$

f) Find a splitting field S of $x^4 - 10x^2 + 21$ over $\mathbb{Q}$. Find $[S : \mathbb{Q}]$ and a basis for S over $\mathbb{Q}$.

Solution. In $\mathbb{Q}[x]$, we have

$$\begin{aligned} x^4 - 10x^2 + 21 &= (x^2 - 7)(x^2 - 3) \\ &= (x + \sqrt{7})(x - \sqrt{7})(x + \sqrt{3})(x - \sqrt{3}) \end{aligned}$$

Therefore, the splitting field S of $x^4 - 10x^2 + 21$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{3}, \sqrt{7})$.

We have

$$\underbrace{[\mathbb{Q}(\sqrt{3}, \sqrt{7}) : \mathbb{Q}]}_{4} = \underbrace{[\mathbb{Q}(\sqrt{3}, \sqrt{7}) : \mathbb{Q}(\sqrt{3})]}_{2} \underbrace{[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}]}_{2}.$$

Finally, notice that $\{1, \sqrt{3}, \sqrt{7}, \sqrt{21}\}$ is a basis for $S = \mathbb{Q}(\sqrt{3}, \sqrt{7})$ over $\mathbb{Q}$. $\square$

Problem 2. (4 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) An algebraically closed field F in which a nonconstant polynomial $f(x) \in F[x]$ has no zero in F.

Solution. No such example exists. We have a proposition that says that a field F is algebraically closed if and only if every nonconstant polynomial in $F[x]$ has a zero in F. $\square$

b) A finite extension field E of F that is not an algebraic extension.

Solution. No such example exists. By a previous theorem, we know that every finite extension field E of F is an algebraic extension. $\square$

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. (Alternatively, 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 PID that is not a UFD.

Solution. No such example exists. We have a theorem that says that every PID is a UFD. □

e) A finite field of characteristic n, where n is a positive integer.

Solution. Take for instance any $\mathbb{Z}_p$, for p a prime. We have a theorem that says that if F is a finite field, then F has characteristic p, where p is a prime. □

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. (10 pts each)

a) Show that $f(x) = x^4 + 4x^2 + 12x + 1$ is irreducible in $\mathbb{Q}[x]$ by an indirect use of Einstenstein's criterion.

Solution. If $f(x)$ were reducible over $\mathbb{Q}$, then so would $f(x + 1)$ be reducible as well, (i.e. if $f(x) = g(x)q(x)$, then we would have that $f(x + 1) = g(x + 1)q(x + 1)$ must also hold). We are going to show the contrapositive of this statement. That is, we are going to use Eisenstein's criterion to show that $f(x + 1)$ is irreducible, from which follows that $f(x)$ must also be irreducible.

We have

$$\begin{aligned} f(x+1) &= (x+1)^4 + 4(x+1)^2 + 12(x+1) + 1 \\ &= (x+1)^2(x+1)^2 + 4(x^2+2x+1) + 12x + 13 \\ &= x^4 + 4x^3 + 10x^2 + 24x + 18 \end{aligned}$$

Now, using Eisenstein's criterion for $p = 2$, we have

- $2 \nmid 1$
- $2 \mid 4, 10, 24, 18$

- $2^2 = 4 \nmid 18$.

Hence, we have that $f(x+1)$ is irreducible over $\mathbb{Q}$, from which follows that $f(x)$ must also be irreducible. $\square$

b) Let $f(x) = 10x^4 + 15x^2 + 9x + 21$. Show that $f(x)$ is irreducible over $\mathbb{Q}$. If α is a zero of $f(x)$ in some extension field of $\mathbb{Q}$, show that $\sqrt[3]{2}$ is not an element of $\mathbb{Q}(\alpha)$.

Solution. Using Eisenstein's criterion for $p = 3$, we have

- $3 \nmid 10$
- $3 \mid 15, 9, 21$
- $3^2 = 9 \nmid 21$.

Hence, $f(x)$ is irreducible over $\mathbb{Q}$, as desired.

Now, let α be a zero of $f(x)$ in some extension field of $\mathbb{Q}$, and assume that $\sqrt[3]{2}$ is an element of $\mathbb{Q}(\alpha)$. Then we have

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\alpha).$$

Thus,

$$\underbrace{[\mathbb{Q}(\alpha) : \mathbb{Q}]}_{4} = \underbrace{[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt[3]{2})}_{?}\underbrace{[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]}_{3}.$$

But $3 \nmid 4$, so we have a contradiction. $(\Rightarrow\Leftarrow)$

Hence, it must be the case that $\sqrt[3]{2} \notin \mathbb{Q}(\alpha)$. $\square$

Problem 4. (26 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, show that $\mathcal{I} = \mathcal{R}$.

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. $\square$

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. $\square$

e) Let E be a splitting field over F of a separable polynomial. Prove that $E_{G(E/F)} = F$.

Proof. To simplify notation, let $G = G(E/F)$. Then we have that $F \subset E_G \subset E$, where

$$E_G = \{\alpha \in E \mid \sigma(\alpha) = \alpha \ \ \forall \sigma \in G\}$$

is a subfield of E. Also, E must be a splitting field of E_G since $|G| = |G(E/F)|$, and by a previous theorem, we know that $|G(E/F)| = [E : F]$[1]. Hence,

$$\begin{aligned} |G| &= [E : F] \\ \implies |G(E/E_G)| &= [E : E_G] \\ \implies [E : F] &= [E : E_G]\,[E_G : F]. \end{aligned}$$

But $[E : F] = [E : E_G]$ by a previous theorem, so must have that $[E_G : F] = 1$, which in turn implies that $E_G = F$, as desired. $\square$

f) Let F be a field and $f(x) \in F[x]$. Prove that $f(x)$ is separable if and only if $f(x)$ and $f'(x)$ are relatively prime.

Proof. ($\Rightarrow$) Let $f(x)$ be separable. Then $f(x)$ factors over some extension field of F as

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n) \qquad \text{where } \alpha_i \neq \alpha_j \quad \text{for } i \neq j.$$

Taking the derivative of $f(x)$, we see that

$$f'(x) = (x - \alpha_2) \cdots (x - \alpha_n) + (x - \alpha_1)(x - \alpha_3) \cdots (x - \alpha_{n-1}).$$

Hence, $f(x)$ and $f'(x)$ can have no common factors, so they are relatively prime.

($\Leftarrow$) Conversely, we want to show that if $f(x)$ and $f'(x)$ are relatively prime, then $f(x)$ is separable. This statement is equivalent to its contrapositive, that is, it is equivalent to saying that if $f(x)$ is not separable, then $f(x)$ and $f'(x)$ are not relatively prime (i.e. $f(x)$ and $f'(x)$ have a common factor). We are going to use this contrapositive argument:

Assume that $f(x)$ is not separable, that is, $f(x)$ has multiple roots. Let

$$f(x) = (x - \alpha)^k \cdot g(x), \qquad \text{where } \ k > 1.$$

Then we have

$$f'(x) = k(x - \alpha)^{k-1} g(x) + g'(x) \cdot (x - \alpha)^k.$$

[1]Here's the theorem, for reference:
Let $f(x)$ be a polynomial in $F[x]$ and suppose that E is a splitting field for $f(x)$ over F. If $f(x)$ has no repeated roots, then we have that $|G(E/F)| = [E : F]$.

Thus, $f(x)$ and $f'(x)$ have a common factor, so they are not relatively prime. $\square$

g) Let E be a field extension of a field F and let $f(x) \in F[x]$. Then any automorphism in $G(E/F)$ defines a permutation of the roots of $f(x)$ that lie in E.

Proof. Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, and suppose that $\alpha \in E$ is a zero of $f(x)$. Then, for $\sigma \in G(E/F)$, we have

$$\begin{aligned} 0 &= \sigma(0) \\ &= \sigma(f(\alpha)) \\ &= \sigma(a_0 + a_1\alpha + \cdots + a_n\alpha^n) \\ &= \sigma(a_0) + \sigma(a_1\alpha) + \cdots + \sigma(a_n\alpha^n) \\ &= a_0 + a_1\sigma(\alpha) + \cdots + a_n\sigma(\alpha^n) \\ &= a_0 + a_1\sigma(\alpha) + \cdots + a_n\sigma(\alpha)^n. \end{aligned}$$

Hence, $\sigma(\alpha)$ is a zero of $f(x)$, and so we have that any automorphism $\sigma \in G(E/F)$ defines a permutation of the roots of $f(x)$ that lie in E. $\square$