MATH 566 – Spring 2024

FINAL EXAM

SOLUTIONS

Prof Arturo Magidin

Part I

I.1 Give an example of each of the following. You do not need to prove that the example has the given properties. *(2 points each, 10 points total)*

(i) A ring R with unity $1_R \neq 0_R$, that has no two-sided ideals other than the trivial and improper ideals, that is other than $\{0_R\}$ and R, but that is not a division ring or field.

Example. One possible example is $\mathsf{M}_{2\times 2}(\mathbb{R})$, the ring of 2×2 matrices with real coefficients. In general, $\mathsf{M}_{n\times n}(F)$ where F is any field and $n > 1$ has this property. $\square$

(ii) A ring R and a one-sided ideal I that is not a two-sided ideal. Specify whether I is a left ideal or a right ideal.

Example. One example is $R = \mathsf{M}_{2\times 2}(\mathbb{R})$, and

$$I = \left\{ \left(\begin{array}{cc} a & b \\ 0 & 0 \end{array} \right) \in R \;\middle|\; a, b \in \mathbb{R} \right\},$$

which is a right ideal but not a left ideal. $\square$

(iii) A division ring that is not a field.

Example. The Hamiltonians $\mathbb{H}$, that is

$$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}, i^2 = j^2 = k^2 = ijk = -1\}$$

are a classical example. $\square$

(iv) A commutative ring R and an ideal I that is not principal.

Example. The ideal (x, y) in $\mathbb{R}[x, y]$ is not principal. $\square$

(v) An integral domain D that is a UFD but not a PID.

Example. The ring $\mathbb{Z}[x]$ is a UFD, as a corollary of Gauss's Lemma, but is not a PID since $(2, x)$ is not a principal ideal. So is $\mathbb{R}[x, y]$. $\square$

I.2 Let D be an integral domain, and let $D[x]$ be the ring of polynomials with coefficients in D.

(i) Prove that (x) is a prime ideal of $D[x]$. *(4 points)*

Proof. The morphism $\varepsilon_0\colon D[x] \to D$ obtained by mapping D to itself via the identity, and sending $x \mapsto 0$, is a surjective ring homomorphism. The kernel are the polynomials with constant term 0; that is, (x). By the First Isomorphism Theorem, $D \cong D[x]/(x)$. Since $D[x]/(x)$ is an integral domain, it follows that (x) is a prime ideal. $\square$

(ii) Prove that (x) is a maximal ideal if and only if D is field. *(3 points)*

Proof. We have that (x) is a maximal ideal if and only if $D[x]/(x)$ is a field, if and only if D is a field. $\square$

(iii) Prove that (x) is not the only nonzero prime ideal of $D[x]$. *(3 points)*

Proof. Since D is an integral domain, $0_R \neq 1_R$. Let $\varepsilon_1\colon D[x] \to D$ be the map obtained by sending D to itself via the identity map, and letting $x \mapsto 1_R$. The kernel of this ideal does not contain x, and contains $x - 1_R \neq 0$; but again we have $D[x]/\ker(\varepsilon_1) \cong D$. So $\ker(\varepsilon_1)$ is a nonzero prime ideal that is different from (x). In fact, this ideal is equal to $(x - 1_R)$, but we do not need to figure this out to know that it is a nonzero prime ideal different from (x). $\square$

I.3 Let R_1 and R_2 be rings with unity. Prove that if I is an ideal of $R_1 \times R_2$, then there exist ideals $J_1 \triangleleft R_1$ and $J_2 \triangleleft R_2$ such that $I = J_1 \times J_2$. *(10 points)*

Proof. Let $\pi_1 \colon R_1 \times R_2 \to R_1$ and $\pi_2 \colon R_1 \times R_2 \to R_2$ be the projections onto the first and second factors, respectively. Let $I \triangleleft R_1 \times R_2$.

Let $J_1 = \pi_1(I)$ and $J_2 = \pi_2(I)$. Since π_i are surjective, by the Lattice Isomorphism Theorem we know that $J_1 \triangleleft R_1$ and $J_2 \triangleleft R_2$ (they are images an ideal, hence an ideal of the image). And if $(a, b) \in I$, then $a \in J_1$ and $b \in J_2$, so $I \subseteq J_1 \times J_2$.

To prove that $J_1 \times J_2 \subseteq I$, let $(r, s) \in J_1 \times J_2$. Then $r \in J_1$, so there exists $y \in R_2$ such that $(r, y) \in I$. Symmetrically, since $s \in J_2$ there exists $x \in R_1$ such that $(x, s) \in I$. Since I is an ideal, sums of products of elements of I with elements of R lie in I, so

$$(r, s) = (r, 0) + (0, s) = (1, 0)(r, y) + (0, 1)(x, s) \in I.$$

Thus, $J_1 \times J_2 \subseteq I$, proving equality. $\square$

I.4 Let $S = \{a \in \mathbb{Z} \mid 2 \nmid a \text{ and } 3 \nmid a\}$ be the set of all integers that are not multiples of 2 or of 3. You may take for granted that this is a multiplicative subset of $\mathbb{Z}$.

Describe all prime ideals of $S^{-1}\mathbb{Z}$. You may invoke theorems from class to verify that the ideals you describe are indeed prime ideals, and that your list is complete. *(10 points)*

Proof. We proved in class that there is a bijection between the prime ideals of $S^{-1}R$ and the prime ideals of R that are disjoint from S, given by mapping such an ideal P of R to the ideal $S^{-1}P = \{\frac{a}{s} \mid a \in P, s \in S\}$ of $S^{-1}R$. So we need to determine the ideals of $\mathbb{Z}$ that are disjoint from S.

The prime ideal (0) is certainly disjoint from S, since $0 \notin S$. A nonzero prime ideal of $\mathbb{Z}$ is of the form (p) with p a positive prime number. If $(p) \cap S = \varnothing$, then $p \notin S$, hence either $2 \mid p$ or $3 \mid p$. But since p is a prime, this means that either $p = 2$ or $p = 3$. Thus, the only nonzero prime ideals that are disjoint from S are (2) and (3).

Thus, $S^{-1}\mathbb{Z}$ has exactly three prime ideals:

$$\begin{aligned}
S^{-1}(0) &= \{0_{S^{-1}\mathbb{Z}}\},\\
S^{-1}(2) &= \left\{ \frac{a}{s} \in S^{-1}\mathbb{Z} \;\middle|\; s \in S, 2 \mid a \right\},\\
S^{-1}(3) &= \left\{ \frac{b}{s} \in S^{-1}\mathbb{Z} \;\middle|\; s \in S, 3 \mid b \right\}. \square
\end{aligned}$$

I.5 Let (R, φ) be a Euclidean domain.

(i) Prove that for every $a \in R - \{0\}$, $\varphi(1_R) \leq \varphi(a)$. *(5 points)*

Proof. If $a \neq 0$, then $1_R a = a \neq 0$. By the properties of the Euclidean function φ, $\varphi(1_R) \leq \varphi(1_R a) = \varphi(a)$. $\square$

(ii) Prove that $a \in R$ is a unit if and only if $a \neq 0$ and $\varphi(a) = \varphi(1_R)$. *(5 points)*

Proof. If a is a unit, then there exists $b \in R$ such that $ab = 1_R$. Then by the properties of the Euclidean function we have $\varphi(a) \leq \varphi(ab) = \varphi(1_R)$. Since we already have that $\varphi(1_R) \leq \varphi(a)$, we obtain equality.

Conversely, if $\varphi(a) = \varphi(1_R)$, then we know that there exist $q, r \in R$ such that $1_R = qa + r$ and either $r = 0$ or $\varphi(r) < \varphi(a) = \varphi(1_R)$. Since there are no nonzero elements with $\varphi(r) < \varphi(1_R)$, we must have $r = 0$, hencer $1_R = qa$. Thus, a is a unit with inverse q. $\square$

Part II

II.1 Give an example of each of the following. You do not need to prove the example has the given properties. *(2 points each, 10 points total)*

(i) Two fields, F and K, such that K is a finite extension of F but K is not a Galois extension of F.

Example. For example, $F = \mathbb{Q}$ and $K = \mathbb{Q}(\sqrt[3]{2})$; or to borrow from problem II.5, $F = \mathbb{Q}$ and $K = \mathbb{Q}(\sqrt[5]{11})$. $\square$

(ii) Two fields, F and K, with K a finitely generated extension of F that is not a finite dimensional extension of F.

Example. One example is $F = \mathbb{Q}$ and $K = \mathbb{Q}(x)$, the field of rational functions over $\mathbb{Q}$. $\square$

(iii) Two fields F and K such that K is an extension of F, and if L is an intermediate extensions, $F \subseteq L \subseteq K$, then either $F = L$ or $L = K$.

Example. Any extension of prime degree will do, so for example $F = \mathbb{Q}$ and $K = \mathbb{Q}(\sqrt{2})$, which has degree 2. $\square$

(iv) Two fields F and K for which there is no nonzero ring homomorphism between them (in either direction).

Example. If $F = \mathbb{Z}_2$ and $K = \mathbb{Z}_3$, then these fields are of different characteristics, so there can be no nonzero ring homomorphism between them: the image of 1_F in K must satisfy that $x + x = 2x = 0$, but that only happens for $x = 0$. And the image of 1_K in F must satisfy $3x = 0$, and this only occurs for $x = 0$.

More generally, there can be no nonzero ring homomorphism between fields of different characteristics. $\square$

(v) A field of characteristic 5 that is infinite.

Example. One example is $\mathbb{Z}_5(x)$, the field of fractions of $\mathbb{Z}_5[x]$. $\square$

II.2 Let $f(x) = x^3 + 2x + 2 \in \mathbb{Q}[x]$, and let α be a root of $f(x)$. Express α^5 and $(\alpha - 1)^{-1}$ in the form $a + b\alpha + c\alpha^2$, with $a, b, c \in \mathbb{Q}$. *(10 points)*

Example. Note that $f(x)$ is irreducible over $\mathbb{Q}$, as it is Einstenstein at 2. So every element of $\mathbb{Q}(\alpha)$ can be written in the form $a + b\alpha + c\alpha^2$.

To express α^5, we divide x^5 by $f(x)$:

$$x^5 = (x^3 + 2x + 2)(x^2 - 2) + (-2x^2 + 4x + 4),$$

so evaluating at α we obtain $\alpha^5 = 4 + 4\alpha - 2\alpha^2$.

To find $(\alpha - 1)^{-1}$, we use the Euclidean Algorithm to express $\gcd(f(x), x - 1)$ in terms of $f(x)$ and $x - 1$. Dividing $f(x)$ by $x - 1$, we get

$$x^3 + 2x + 2 = (x^2 + x + 3)(x - 1) + 5.$$

This means that:

$$\begin{aligned} 5 &= (x^3 + 2x + 2) - (x^2 + x + 3)(x - 1) \\ 1 &= \frac{1}{5}(x^3 + 2x + 2) - \left(\frac{1}{5}x^2 + \frac{1}{5}x + \frac{3}{5}\right)(x - 1). \end{aligned}$$

Evaluating at α, we obtain

$$1 = (\alpha - 1)\left(-\frac{3}{5} - \frac{1}{5}\alpha - \frac{1}{5}\alpha^2\right),$$

so $(\alpha - 1)^{-1} = -\frac{3}{5} - \frac{1}{5}\alpha - \frac{1}{5}\alpha^2$. $\square$

II.3 (i) Let K be a finite dimensional Galois extension of F. Prove that there are only finitely many intermediate extensions; that is, fields L such that $F \subseteq L \subseteq K$. *(5 points)*

Proof. By the Fundamental Theorem of Galois Theory, there is a one-to-one, inclusion reversing correspondence between the subgroups of $\mathrm{Gal}(K/F)$ and the intermediate extensions. Since $\mathrm{Gal}(K/F)$ is finite, it has only finitely many subgroups, so there are only finitely many intermediate extensions. $\square$

(ii) Let K be a finite dimensional Galois extension of F. Prove that if $\mathrm{Gal}(K/F)$ is an abelian group, then every intermediate extension L is Galois over F. That is, if L is a field such that $F \subseteq L \subseteq K$, then L is Galois over F. *(5 points)*

Proof. By the Fundamental Theorem of Galois Theory, a subextension L is Galois over F if and only if $\mathrm{Aut}_L(K)$ is a normal subgroup of $\mathrm{Gal}(K/F)$. If $\mathrm{Gal}(K/F)$ is abelian, then *every* subgroup is normal, so that means that every intermediate extension L is Galois over F. $\square$

II.4 Let K be an extension of F, and let $\alpha \in K$. Prove that if $[F(\alpha) : F]$ is finite, then α is algebraic over F. *(10 points)*

Proof. Let $[F(\alpha) : F] = n$. Then $1, \alpha, \ldots, \alpha^n$ are $n+1$ elements of K, which has dimension n as a vector space over F. That means that they are linearly dependent over F, so there exist $a_0, \ldots, a_n \in F$, not all zero, such that $a_0 1 + \cdots + a_n\alpha^n = 0$. Let $f(x) \in F[x]$ be the polynomial

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n.$$

Then $f(x) \neq 0$, $f(x) \in F[x]$, and $f(\alpha) = 0$. Thus, α is algebraic over F, as claimed.

II.5 Let $K = \mathbb{Q}(\sqrt[5]{11})$, where $\sqrt[5]{11}$ is the real positive fifth root of 11.

(i) Find $[K : \mathbb{Q}]$. *(3 points)*

Answer. Note that $\sqrt[5]{11}$ is a root of $f(x) = x^5 - 11$. This polynomial is irreducible in $\mathbb{Q}$ by Eisenstein's Criterion at $p = 11$, so this is the monic irreducible polynomial of $\sqrt[5]{11}$ over $\mathbb{Q}$. Therefore,

$$[K : \mathbb{Q}] = \deg(f) = 5.$$

(ii) Describe explicitly all elements of $\mathrm{Aut}_{\mathbb{Q}}(K)$. *(4 points)*

Answer. An automorphism of K over $\mathbb{Q}$ must send every rational to itself, and so is completely determined by its value on $\sqrt[5]{11}$. The image of $\sqrt[5]{11}$ must be a root of $x^5 - 11$ in K. But $x^5 - 11$ has one real root and four nonreal roots, and $K \subseteq \mathbb{R}$. So $\sqrt[5]{11}$ is the only root of $f(x)$ that lies in K. That means that if $\varphi \in \mathrm{Aut}_{\mathbb{Q}}(K)$, then $\varphi(q) = q$ for all $q \in \mathbb{Q}$, and $\varphi(\sqrt[5]{11}) = \sqrt[5]{11}$. Thus, $\varphi = \mathrm{id}_K$.

Thus we have shown that $\mathrm{Aut}_{\mathbb{Q}}(K) = \{\mathrm{id}_K\}$. $\square$n

(iii) Is K a Galois extension of $\mathbb{Q}$? Justify your answer. *(3 points)*

Answer. K is a Galois extension of $\mathbb{Q}$ if and only if the fixed field of $\mathrm{Aut}_{\mathbb{Q}}(K)$ is $\mathbb{Q}$. Since $\mathrm{Aut}_{\mathbb{Q}}(K) = \{\mathrm{id}_K\}$, the fixed field is $\{\mathrm{id}_K\}' = K \neq \mathbb{Q}$. So K is not a Galois extension of $\mathbb{Q}$. $\square$