Math 415B/515B - Intro to Abstract Algebra — Instructor: Jay Taylor
Spring 2019

Final Exam - Study Guide

Rings, Subrings, and Ideals

Question 1
Assume R and S are rings and let $\mathrm{Fun}(R, S)$ be the set of all functions $f : R \to S$. Show that $\mathrm{Fun}(R, S)$ is a ring with the addition and multiplication defined by

$$(f+g)(r) = f(r) + g(r) \qquad (fg)(r) = f(r)g(r)$$

for all $f, g \in \mathrm{Fun}(R, S)$ and $r \in R$.

Question 2
Let R be a ring. The *center* of R is defined to be $Z(R) = \{r \in R \mid ra = ar \text{ for all } a \in R\}$. Show that $Z(R)$ is a subring of R.

Question 3
Recall that an element $e \in R$ in a ring R is called an *idempotent* if $e^2 = e$. Determine all the idempotents in $\mathbb{Z}^n = \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$ (n copies of $\mathbb{Z}$).

Question 4
Assume $I, J \subseteq R$ are ideals of a ring R. Show that $I + J = \{x + y \mid x \in I, y \in J\} \subseteq R$ is an ideal.

Question 5
Assume $I, J \subseteq R$ are ideals of a ring R. Show that $IJ = \bigcup_{n \in \mathbb{N}_0} (IJ)_n$ is an ideal where $(IJ)_n = \{a_1b_1 + \cdots + a_nb_n \mid a_i \in I \text{ and } b_i \in J\}$.

Question 6
Let R be a ring and $A \subseteq R$ a *subset*. Show that

$$\langle A \rangle = \bigcap_{A \subseteq I \subseteq R} I$$

is an ideal of R where the intersection is taken over all ideals $I \subseteq R$ containing A.

Question 7
Let $A = \{a_1, \ldots, a_n\} \subseteq R$ be a finite subset of a unital ring R. Show that $\langle A \rangle = \{r_1 a_1 s_1 + \cdots + r_n a_n s_n \mid r_i, s_i \in R\}$.

Question 8
Let R be an integral domain and $n > 0$ an integer. Denote by $I \subseteq R[X]$ the set of polynomials $f = \sum_{i \in \mathbb{N}_0} a_i X^i$ where either $f = 0$ or $\deg(f) \geqslant n$. Show that I is a principal ideal of $R[X]$.

Question 9
let R be a commutative ring and $I \subseteq R$ an ideal. Show that the annihilator of I

$$\mathrm{Ann}(I) = \{r \in R \mid ra = 0 \text{ for all } a \in I\}$$

is also an ideal of R.

Question 10
let R be a commutative ring and $I \subseteq R$ an ideal. Show that the nil radical of I

$$\mathrm{NilRad}(I) = \{r \in R \mid r^n \in I \text{ for some integer } n > 0 \text{ depending on } r\}$$

is also an ideal of R.

Question 11
Prove that the set of all polynomials whose coefficients are all even is a prime ideal of $\mathbb{Z}[X]$.

Homomorphisms

Question 12
Assume $\phi : R \to S$ is a homomorphism of rings. Show that the following hold:

(i) If $I \subseteq R$ is an ideal of R then $\phi(I) \subseteq S$ is an ideal of S.

(ii) If $K \subseteq S$ is an ideal of S then $\phi^{-1}(K) = \{r \in R \mid \phi(r) \in K\} \subseteq R$ is an ideal of R.

Question 13
Assume $\phi : R \to S$ is a homomorphism of rings. Show that if $I \subseteq S$ is a prime ideal of S then $\phi^{-1}(I) = \{r \in R \mid \phi(r) \in I\} \subseteq R$ is a prime ideal of R.

Question 14
Assume R is a unital ring. Show that R contains a subring $S \subseteq R$, with $1_R \in S$, such that S is isomorphic to either $\mathbb{Z}$ or $\mathbb{Z}/n\mathbb{Z}$ for some integer $n > 0$.

Question 15
Let $n \geqslant 0$ be an integer with decimal representation $a_k a_{k-1} \cdots a_1 a_0$. For example, if $n = 2513$ then $k = 3$ and $(a_3, a_2, a_1, a_0) = (2, 5, 1, 3)$. Prove that n is divisible by 11 if and only if $a_0 - a_1 + a_2 - \cdots - (-1)^k a_k$ is divisible by 11.

Question 16
Let $\phi : R \to S$ be a ring homomorphism. Show that ϕ is an isomorphism if and only if ϕ is surjective and $\mathrm{Ker}(\phi) = \{0\}$.

Question 17
Prove that $\mathbb{Q}[X]/\langle X^2 - 2\rangle$ is isomorphic to $\mathbb{Q}[\sqrt{2}] = \{a + \sqrt{2}b \mid a, b \in \mathbb{Q}\}$.

Question 18
Show that if $u \in U(R)$ is a unit in a unital commutative ring R then u is not a zero divisor. Moreover, show that every element in $\mathbb{Z}_n$, with $n > 0$ an integer, is either a unit or a zero divisor.

Question 19
Assume $\phi : R \to S$ is a ring homomorphism and $I \subseteq R$ is an ideal with $I \subseteq \mathrm{Ker}(\phi)$. Show that the function $\bar{\phi} : R/I \to S$, defined by $\bar{\phi}(r + I) = \phi(r)$, is a well-defined ring

homomorphism.

Question 20
Assume $k, m, n > 0$ are integers such that $kn \in m\mathbb{Z}$ and $k^2 - k \in m\mathbb{Z}$. Show that $\psi_k : \mathbb{Z}_n \to \mathbb{Z}_m$, defined by $\psi_k(x + n\mathbb{Z}) = kx + m\mathbb{Z}$, is a ring homomorphism.

Question 21
Determine all the ring homomorphisms $\mathbb{Z}_{15} \to \mathbb{Z}_{12}$. Are any of these homomorphisms surjective?

Question 22
Determine all the ring homomorphisms $\mathbb{Z} \oplus \mathbb{Z} \to \mathbb{Z}$.

Question 23
Let R be a commutative ring of prime characteristic $p > 0$ and let $F : R \to R$ be the Frobenius endomorphism defined by $F(x) = x^p$. Show that the following hold:

(i) F is a ring homomorphism,

(ii) if R is finite then F is a bijection.

Question 24
Assume R is a ring, $S \subseteq R$ is a subring, and $I \subseteq R$ is an ideal. Show that we have an isomorphism $S/(S \cap I) \cong (S + I)/I$.

Polynomial Rings

Question 25
Assume $\mathbb{F}$ is a field and $a \in \mathbb{F}$. Show that $X - a$ divides $f \in \mathbb{F}[X]$ if and only if $f(a) = 0$.

Question 26
Assume R and S are rings and $\phi : R \to S$ is a ring homomorphism. Show that this extends to a ring homomorphism $\bar{\phi} : R[X] \to S[X]$ defined by

$$\bar{\phi}\left(\sum_{i \in \mathbb{N}_0} a_i X^i\right) = \sum_{i \in \mathbb{N}_0} \phi(a_i) X^i.$$

Question 27
Let R be a ring and $I \subseteq R$ an ideal. Show that $I[X] \subseteq R[X]$ is an ideal of $R[X]$ and we have an isomorphism $R[X]/I[X] \cong (R/I)[X]$.

Question 28
Let $f = 5X^4 + 3X^3 + 1 \in \mathbb{F}_7[X]$ and $g = 3X^2 + 2X + 1 \in \mathbb{F}_7[X]$. Determine the quotient and remainder upon diving f by g.

Question 29
Let R be a ring and $f, g \in R[X]$ non-zero polynomials. Show that if R is an integral domain then $\deg(fg) = \deg(f) + \deg(g)$. Give an example of a ring R and non-zero polynomials $f, g \in R[X]$ such that $\deg(fg) < \deg(f) + \deg(g)$.

Question 30
Let $\mathbb{F}$ be a field and $p \in \mathbb{F}[X]$ a non-zero polynomial of degree $n \geqslant 0$. Show that

$$\{X^0 + \langle p \rangle, X^1 + \langle p \rangle, \ldots, X^{n-1} + \langle p \rangle\}$$

is a basis of the $\mathbb{F}$-vector space $\mathbb{F}[X]/\langle p \rangle$.

Question 31
Assume $\mathbb{F}$ is a finite field of characteristic $p > 0$. Show that there exists an element $\alpha \in \mathbb{F}$ such that the polynomial $X^p - X - \alpha \in \mathbb{F}[X]$ has no zeros in $\mathbb{F}$.

Question 32
Assume R is a UFD and let $\mathbb{F}$ be the field of fractions of R. Show that if $f \in R[X]$ is primitive and irreducible over $\mathbb{F}$ then f is irreducible.

Question 33
Assume R is a UFD.

(i) Define what it means for a polynomial $f \in R[X]$ to be primitive.

(ii) Show that if $f, g \in R[X]$ are primitive then $fg \in R[X]$ is primitive.

Question 34
Find all monic irreducible polynomials of degree 2 over $\mathbb{F}_3$.

Question 35
Show that if an integer $n > 0$ can be written in the form t^2m then $tmX + 1$ is a unit in $\mathbb{Z}_n[X]$.

Question 36
For any integer $m > 0$ let $\Phi_m \in \mathbb{Z}[X]$ denote the m^{th} cyclotomic polynomial. Assume that $n = 2p$ with $p > 0$ an odd prime. Show that $\Phi_{2p}(X) = \Phi_p(-X)$.

Question 37
Compute the cyclotomic polynomial Φ_{12}.

Question 38
Show that the polynomial $X^4 + X + 1 \in \mathbb{Z}[X]$ is irreducible over $\mathbb{Z}$.

Question 39
Let $\mathbb{F}$ be a field and $f \in \mathbb{F}[X]$ a non-zero polynomial. Denote by $\partial_X(f) \in \mathbb{F}[X]$ is the derivative of f. Show that f has a multiple zero if and only if $\gcd(f, \partial_X(f)) \neq 1$.

EDs, PIDs, and UFDs

Question 40
Prove that $\mathbb{Z}[X]$ is not a PID.

Question 41
Assume $\mathbb{F}$ is a field. Show that $\mathbb{F}[X]$ is a PID. Is $\mathbb{F}[X]$ a UFD?

Question 42
Assume R is a PID. Show that $f \in R$ is irreducible if and only if $\langle f \rangle \subseteq R$ is a maximal ideal.

Question 43
Show that the homomorphic image of a PID is a PID.

Question 44
Let $f = X^2 + 1 \in \mathbb{Z}[X]$. Prove that the ideal $\langle f \rangle \subseteq \mathbb{Z}[X]$ is prime but not maximal.

Question 45
In $\mathbb{Z}[\sqrt{-5}]$ prove that $1+3\sqrt{-5}$ is irreducible but not prime. Is $\mathbb{Z}[\sqrt{-5}]$ a PID?

Question 46
In $\mathbb{Z}[\sqrt{5}]$ prove that both 2 and $1+\sqrt{5}$ are irreducible but not prime.

Question 47
Let $R = \mathbb{Z}[\sqrt{-7}]$ and let $N : R \to \mathbb{N}_0$ be the function defined by $N(a+b\sqrt{-7}) = a^2+7b^2$. Show that $N(6+2\sqrt{-7}) = N(1+3\sqrt{-7})$ but $6+2\sqrt{-7}$ and $1+3\sqrt{-7}$ are not associates.

Question 48
In the Gaussian integers $\mathbb{Z}[i]$ show that 3 is irreducible but 2 and 5 are not.

Question 49
Let $R = \mathbb{Z}[i]$ and let $d : R \to \mathbb{N}_0$ be the function defined by $d(a+bi) = a^2+b^2$. Find elements $q, r \in R$ such that $3-4i = (2+5i)q + r$ and $d(r) < d(2+5i)$.

Question 50
Let $R = \mathbb{Z}[\sqrt{2}]$ and let $d : R \to \mathbb{N}_0$ be the function defined by $d(a+b\sqrt{2}) = |a^2-2b^2|$. Find $q, r \in \mathbb{Z}[\sqrt{2}]$ such that $2+7\sqrt{2} = (1-\sqrt{2})q + r$ and $d(r) < d(1-\sqrt{2})$.

Question 51
Assume (R, d) is a Euclidean domain and $I \subseteq R$ is a non-zero ideal. Show that for $0 \neq g \in I$ the following are equivalent:

(i) $d(g) \leqslant d(h)$ for all $h \in I$,

(ii) $I = \langle g \rangle$.

Conclude that R is a PID.

Fields

Question 52
Prove that if $\mathbb{F}$ is a finite field with $|\mathbb{F}| = q$ then $\mathbb{F}$ is a splitting field for $X^q - X$.

Question 53
Construct a finite field of size $729 = 9^3$.

Question 54
Let $\mathbb{F}$ be the field of fractions of the Gaussian integers $\mathbb{Z}[i]$. Prove that we have an isomorphism $\mathbb{F} \cong \mathbb{Q}(i)$.

Question 55
Find the minimal polynomial $p \in \mathbb{Q}[X]$ of $\sqrt{1+\sqrt{5}} \in \mathbb{R}$ over $\mathbb{Q}$. What's the degree $[\mathbb{Q}(\sqrt{1+\sqrt{5}}) : \mathbb{Q}]$?

Question 56
Find the minimal polynomial of $\sqrt[3]{2} + \sqrt[3]{4}$ over $\mathbb{Q}$.

Question 57
Show that $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) = \mathbb{Q}(\sqrt[6]{2})$.

Question 58
Show that for any $a, b \in \mathbb{Q}$ we have $\mathbb{Q}(\sqrt{a}, \sqrt{b}) = \mathbb{Q}(\sqrt{a} + \sqrt{b})$.

Question 59
Suppose $\mathbb{Q} \subseteq F \subseteq \mathbb{C}$ is a field extension with $[F : \mathbb{Q}] = 2$. Show that there exists a $d \in \mathbb{Z}$ such that $F = \mathbb{Q}(\sqrt{d})$.

Question 60
Let F be a field and $f \in F[X]$ a non-zero polynomial with $\deg(f) = 2$. Assume $F \subseteq E$ is a field extension containing a zero $\alpha \in E$ of f. Show that $F(\alpha) \subseteq E$ is a splitting field of f.

Question 61
Let $K = \mathbb{Q}(\sqrt{7}, i)$. Show that the following hold:

(i) K is a splitting field over $\mathbb{Q}$ for $X^4 - 6X^2 - 7 \in \mathbb{Q}[X]$.

(ii) $[K : \mathbb{Q}] = 4$.

Question 62
Let $a \in \mathbb{C}$ be a zero of $X^2 + X + 1 \in \mathbb{Q}[X]$. Prove that $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(a)$.