Algebra Qualifying Exam Questions

D. Zack Garza

Sunday 26^{th} July, 2020

Contents

1 Spring 2020

1.1 1

a. Show that any group of order 2020 is solvable.

b. Give (without proof) a classification of all abelian groups of order 2020.

c. Describe one nonabelian group of order 2020.

1.2 2

Let H be a normal subgroup of a finite group G where the order of H and the index of H in G are relatively prime. Prove that no other subgroup of G has the same order as H.

1.3 3

Let E be an extension field of F and $\alpha \in E$ be algebraic of odd degree over F.

a. Show that $F(\alpha) = F(\alpha^2)$.

b. Prove that α^{2020} is algebraic of odd degree over F.

1.4 4

Let $f(x) = x^4 - 2 \in \mathbb{Q}[x]$.

a. Define what it means for a finite extension field E of a field F to be a Galois extension.

b. Determine the Galois group $\mathrm{Gal}(E/\mathbb{Q})$ for the polynomial $f(x)$, and justify your answer carefully.

c. Exhibit a subfield K in (b) such that $\mathbb{Q} \leq K \leq E$ with K not a Galois extension over $\mathbb{Q}$. Explain.

1.5 5

Let R be a ring and $f : M \longrightarrow N$ and $g : N \longrightarrow M$ be R-module homomorphisms such that $g \circ f = \mathrm{id}_M$. Show that $N \cong \operatorname{im} f \oplus \ker g$.

1.6 6

Let R be a ring with unity.

a. Give a definition for a free module over R.

b. Define what it means for an R-module to be torsion free.

c. Prove that if F is a free module, then any short exact sequence of R-modules of the following form splits:

$$0 \longrightarrow N \longrightarrow M \longrightarrow F \longrightarrow 0.$$

d. Let R be a PID. Show that any finitely generated R-module M can be expressed as a direct sum of a torsion module and a free module. You may assume that a finitely generated torsionfree module over a PID is free.

1.7 7

Let

$$A = \begin{bmatrix} 2 & 0 & 0 \\ 4 & 6 & 1 \\ -16 & -16 & -2 \end{bmatrix} \in M_3(\mathrm{C}).$$

a. Find the Jordan canonical form J of A.

b. Find an invertible matrix P such that $P^{-1}AP = J$. You should not need to compute P^{-1}.

c. Write down the minimal polynomial of A.

1.8 8

Let $T : V \longrightarrow V$ be a linear transformation where V is a finite-dimensional vector space over $\mathbb{C}$. Prove the Cayley-Hamilton theorem: if $p(x)$ is the characteristic polynomial of T, then $p(T) = 0$. You may use canonical forms.

2 Fall 2019

2.1 1

Let G be a finite group with n distinct conjugacy classes. Let $g_1 \cdots g_n$ be representatives of the conjugacy classes of G.

Prove that if $g_i g_j = g_j g_i$ for all i, j then G is abelian.

2.2 2

Let G be a group of order 105 and let P, Q, R be Sylow 3, 5, 7 subgroups respectively.

(a) Prove that at least one of Q and R is normal in G.

(b) Prove that G has a cyclic subgroup of order 35.

(c) Prove that both Q and R are normal in G.

(d) Prove that if P is normal in G then G is cyclic.

2.3 3

Let R be a ring with the property that for every $a \in R, a^2 = a$.

(a) Prove that R has characteristic 2.

(b) Prove that R is commutative.

2.4 4

Let F be a finite field with q elements.

Let n be a positive integer relatively prime to q and let ω be a primitive nth root of unity in an extension field of F.

Let $E = F[\omega]$ and let $k = [E : F]$.

(a) Prove that n divides $q^k - 1$.

(b) Let m be the order of q in $\mathbb{Z}/n\mathbb{Z}$. Prove that m divides k.

(c) Prove that $m = k$.

2.5 5

Let R be a ring and M an R-module.

> Recall that the set of torsion elements in M is defined by
>
> $$\mathrm{Tor}(m) = \{m \in M \mid \exists r \in R,\ r \neq 0,\ rm = 0\}.$$

(a) Prove that if R is an integral domain, then $\mathrm{Tor}(M)$ is a submodule of M .

(b) Give an example where $\mathrm{Tor}(M)$ is not a submodule of M.

(c) If R has zero-divisors, prove that every non-zero R-module has non-zero torsion elements.

2.6 6

Let R be a commutative ring with multiplicative identity. Assume Zorn's Lemma.

(a) Show that

$$N = \{r \in R \mid r^n = 0 \text{ for some } n > 0\}$$

is an ideal which is contained in any prime ideal.

(b) Let r be an element of R not in N. Let S be the collection of all proper ideals of R not containing any positive power of r. Use Zorn's Lemma to prove that there is a prime ideal in S.

(c) Suppose that R has exactly one prime ideal P . Prove that every element r of R is either nilpotent or a unit.

2.7 7

Let ζ_n denote a primitive nth root of $1 \in \mathbb{Q}$. You may assume the roots of the minimal polynomial $p_n(x)$ of ζ_n are exactly the primitive nth roots of 1.

Show that the field extension $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$ is Galois and prove its Galois group is $(\mathbb{Z}/n\mathbb{Z})^\times$.

How many subfields are there of $\mathbb{Q}(\zeta_{20})$?

2.8 8

Let $\{e_1, \cdots, e_n\}$ be a basis of a real vector space V and let

$$\Lambda := \left\{ \sum r_i e_i \;\middle|\; r_i \in \mathbb{Z} \right\}$$

Let $\cdot$ be a non-degenerate ($v \cdot w = 0$ for all $w \in V \iff v = 0$) symmetric bilinear form on V such that the Gram matrix $M = (e_i \cdot e_j)$ has integer entries.

Define the dual of Λ to be

$$\Lambda^\vee := \{v \in V \;\big|\; v \cdot x \in \mathbb{Z} \text{ for all } x \in \Lambda\}.$$

(a) Show that $\Lambda \subset \Lambda^\vee$.

(b) Prove that $\det M \neq 0$ and that the rows of M^{-1} span $\Lambda^\vee$.

(c) Prove that $\det M = |\Lambda^\vee / \Lambda|$.

3 2019 Course Exams

3.1 Midterm

1. Let G be a group of order $p^2 q$ for p, q prime. Show that G has a nontrivial normal subgroup.
2. Let G be a finite group and let P be a sylow p-subgroup for p prime. Show that $N(N(P)) = N(P)$ where N is the normalizer in G.
3. Show that there exist no simple groups of order 148.
4. Let p be a prime. Show that $S_p = \langle \tau, \sigma \rangle$ where τ is a transposition and σ is a p-cycle.
5. Let G be a nonabelian group of order p^3 for p prime. Show that $Z(G) = [G, G]$
6. Compute the Galois group of $f(x) = x^3 - 3x - 3 \in \mathbb{Q}[x]/\mathbb{Q}$.
7. Show that a field k of characteristic $p \neq 0$ is perfect $\iff$ for every $x \in k$ there exists a $y \in k$ such that $y^p = x$.
8. Let k be a field of characteristic $p \neq 0$ and $f \in k[x]$ irreducible. Show that $f(x) = g(x^{p^d})$ where $g(x) \in k[x]$ is irreducible and separable. Concluded that every root of f has the same multiplicity p^d in the splitting field of f over k.
9. Let $n \geq 3$ and ζ_n be a primitive nth root of unity. Show that $[\mathbb{Q}(\zeta_n + \zeta_n^{-1}) : \mathbb{Q}] = \varphi(n)/2$ for φ the totient function.
10. Let L/K be a finite normal extension

- Show that if L/K is cyclic and E/K is normal with $L/E/K$ then L/E and E/K are cyclic.
- Show that if L/K is cyclic then there exists exactly one extension E/K of degree n with $L/E/K$ for each divisor n of $[L : K]$.

3.2 Final

1. Let A be an abelian group, and show A is a $\mathbb{Z}$-module in a unique way.
2. Consider the $\mathbb{Z}$-submodule N of $\mathbb{Z}^3$ spanned by $f_1 = [-1, 0, 1], f_2 = [2, -3, 1], f_3 = [0, 3, 1], f_4 = [3, 1, 5]$. Find a basis for N and describe $\mathbb{Z}^3/N$.

3. Let $R = k[x]$ for k a field and let M be the R-module given by

$$M = \frac{k[x]}{(x-1)^3} \oplus \frac{k[x]}{(x^2+1)^2} \oplus \frac{k[x]}{(x-1)\left(x^2+1\right)^4} \oplus \frac{k[x]}{(x+2)\left(x^2+1\right)^2}.$$

Describe the elementary divisors and invariant factors of M.

4. Let $I = (2, x)$ be an ideal in $R = \mathbb{Z}[x]$, and show that I is not a direct sum of nontrivial cyclic R-modules.
5. Let R be a PID.

- Classify irreducible R-modules up to isomorphism.
- Classify indecomposable R-modules up to isomorphism.

6. Let V be a finite-dimensional k-vector space and $T : V \longrightarrow V$ a non-invertible k-linear map. Show that there exists a k-linear map $S : V \longrightarrow V$ with $T \circ S = 0$ but $S \circ T \neq 0$.
7. Let $A \in M_n(\mathbb{C})$ with $A^2 = A$. Show that A is similar to a diagonal matrix, and exhibit an explicit diagonal matrix similar to A.
8. Exhibit the rational canonical form for

- $A \in M_6(\mathbb{Q})$ with minimal polynomial $(x-1)(x^2+1)^2$.
- $A \in M_{10}(\mathbb{Q})$ with minimal polynomial $(x^2+1)^2(x^3+1)$.

9. Exhibit the rational and Jordan canonical forms for the following matrix $A \in M_4(\mathbb{C})$:

$$A = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ -2 & -2 & 0 & 1 \\ -2 & 0 & -1 & -2 \end{pmatrix}.$$

10. Show that the eigenvalues of a Hermitian matrix A are real and that $A = PDP^{-1}$ where P is an invertible matrix with orthogonal columns.

4 Spring 2019

4.1 1.

Let A be a square matrix over the complex numbers. Suppose that A is nonsingular and that A^{2019} is diagonalizable over $\mathbb{C}$.

Show that A is also diagonalizable over $\mathbb{C}$.

4.2 2.

Let $F = \mathbb{F}_p$, where p is a prime number.

(a) Show that if $\pi(x) \in F[x]$ is irreducible of degree d, then $\pi(x)$ divides $x^{p^d} - x$.

(b) Show that if $\pi(x) \in F[x]$ is an irreducible polynomial that divides $x^{p^n} - x$, then $\deg \pi(x)$ divides n.

4.3 3.

How many isomorphism classes are there of groups of order 45?

Describe a representative from each class.

4.4 4.

For a finite group G, let $c(G)$ denote the number of conjugacy classes of G.

(a) Prove that if two elements of G are chosen uniformly at random,then the probability they commute is precisely

$$\frac{c(G)}{|G|}.$$

(b) State the class equation for a finite group.

(c) Using the class equation (or otherwise) show that the probability in part (a) is at most

$$\frac{1}{2} + \frac{1}{2[G : Z(G)]}.$$

Here, as usual, $Z(G)$ denotes the center of G.

4.5 5.

Let R be an integral domain. Recall that if M is an R-module, the *rank* of M is defined to be the maximum number of R-linearly independent elements of M .

(a) Prove that for any R-module M, the rank of $\mathrm{Tor}(M)$ is 0.

(b) Prove that the rank of M is equal to the rank of of $M/\mathrm{Tor}(M)$.

(c) Suppose that M is a non-principal ideal of R.

Prove that M is torsion-free of rank 1 but not free.

4.6 6.

Let R be a commutative ring with 1.

Recall that $x \in R$ is nilpotent iff $xn = 0$ for some positive integer n.

(a) Show that every proper ideal of R is contained within a maximal ideal.

(b) Let $J(R)$ denote the intersection of all maximal ideals of R.

Show that $x \in J(R) \iff 1 + rx$ is a unit for all $r \in R$.

(c) Suppose now that R is finite. Show that in this case $J(R)$ consists precisely of the nilpotent elements in R.

4.7 7.

Let p be a prime number. Let A be a $p \times p$ matrix over a field F with 1 in all entries except 0 on the main diagonal.

Determine the Jordan canonical form (JCF) of A

(a) When $F = \mathbb{Q}$,

(b) When $F = \mathbb{F}_p$.

> Hint: In both cases, all eigenvalues lie in the ground field. In each case find a matrix P such that $P^{-1}AP$ is in JCF.

4.8 8.

Let $\zeta = e^{2\pi i/8}$.

(a) What is the degree of $\mathbb{Q}(\zeta)/\mathbb{Q}$?

(b) How many quadratic subfields of $\mathbb{Q}(\zeta)$ are there?

(c) What is the degree of $\mathbb{Q}(\zeta, \sqrt[4]{2})$ over $\mathbb{Q}$?

5 Fall 2018

5.1 1.

Let G be a finite group whose order is divisible by a prime number p. Let P be a normal p-subgroup of G (so $|P| = p^c$ for some c).

(a) Show that P is contained in every Sylow p-subgroup of G.

(b) Let M be a maximal proper subgroup of G. Show that either $P \subseteq M$ or $|G/M| = p^b$ for some $b \leq c$.

5.2 2.

(a) Suppose the group G acts on the set X . Show that the stabilizers of elements in the same orbit are conjugate.

(b) Let G be a finite group and let H be a proper subgroup. Show that the union of the conjugates of H is strictly smaller than G, i.e.

$$\bigcup_{g \in G} gHg^{-1} \subsetneq G$$

(c) Suppose G is a finite group acting transitively on a set S with at least 2 elements. Show that there is an element of G with no fixed points in S.

5.3 3.

Let $F \subset K \subset L$ be finite degree field extensions. For each of the following assertions, give a proof or a counterexample.

(a) If L/F is Galois, then so is K/F.

(b) If L/F is Galois, then so is L/K.

(c) If K/F and L/K are both Galois, then so is L/F.

5.4 4.

Let V be a finite dimensional vector space over a field (the field is not necessarily algebraically closed).

Let $\varphi : V \longrightarrow V$ be a linear transformation. Prove that there exists a decomposition of V as $V = U \oplus W$, where U and W are φ-invariant subspaces of V , $\varphi|_U$ is nilpotent, and $\varphi|_W$ is nonsingular.

5.5 5.

Let A be an $n \times n$ matrix.

(a) Suppose that v is a column vector such that the set $\{v, Av, ..., A^{n-1}v\}$ is linearly independent. Show that any matrix B that commutes with A is a polynomial in A.

(b) Show that there exists a column vector v such that the set $\{v, Av, ..., A^{n-1}v\}$ is linearly independent $\iff$ the characteristic polynomial of A equals the minimal polynomial of A.

5.6 6.

Let R be a commutative ring, and let M be an R-module. An R-submodule N of M is maximal if there is no R-module P with $N \subsetneq P \subsetneq M$.

(a) Show that an R-submodule N of M is maximal $\iff$ M/N is a simple R-module: i.e., M/N is nonzero and has no proper, nonzero R-submodules.

(b) Let M be a $\mathbb{Z}$-module. Show that a $\mathbb{Z}$-submodule N of M is maximal $\iff$ $\#M/N$ is a prime number.

(c) Let M be the $\mathbb{Z}$-module of all roots of unity in $\mathbb{C}$ under multiplication. Show that there is no maximal $\mathbb{Z}$-submodule of M.

5.7 7.

Let R be a commutative ring.

(a) Let $r \in R$. Show that the map

$$\begin{aligned} r\bullet : R &\longrightarrow R \\ x &\mapsto rx. \end{aligned}$$

is an R-module endomorphism of R.

(b) We say that r is a **zero-divisor** if r$\bullet$ is not injective. Show that if r is a zero-divisor and $r \neq 0$, then the kernel and image of R each consist of zero-divisors.

(c) Let $n \geq 2$ be an integer. Show: if R has exactly n zero-divisors, then $\#R \leq n^2$.

(d) Show that up to isomorphism there are exactly two commutative rings R with precisely 2 zero-divisors.

You may use without proof the following fact: every ring of order 4 is isomorphic to exactly one of the following:

$$\frac{\mathbb{Z}}{4\mathbb{Z}}, \quad \frac{\frac{\mathbb{Z}}{2\mathbb{Z}}[t]}{(t^2+t+1)}, \quad \frac{\frac{\mathbb{Z}}{2\mathbb{Z}}[t]}{(t^2-t)}, \quad \frac{\frac{\mathbb{Z}}{2\mathbb{Z}}[t]}{(t^2)}.$$

6 Spring 2018

6.1 1.

(a) Use the Class Equation (equivalently, the conjugation action of a group on itself) to prove that any p-group (a group whose order is a positive power of a prime integer p) has a nontrivial center.

(b) Prove that any group of order p^2 (where p is prime) is abelian.

(c) Prove that any group of order $5^2 \cdot 7^2$ is abelian.

(d) Write down exactly one representative in each isomorphism class of groups of order $5^2 \cdot 7^2$.

6.2 2.

Let $f(x) = x^4 - 4x^2 + 2 \in \mathbb{Q}[x]$.

(a) Find the splitting field K of f, and compute $[K : \mathbb{Q}]$.

(b) Find the Galois group G of f, both as an explicit group of automorphisms, and as a familiar abstract group to which it is isomorphic.

(c) Exhibit explicitly the correspondence between subgroups of G and intermediate fields between $\mathbb{Q}$ and k.

6.3 3.

Let K be a Galois extension of $\mathbb{Q}$ with Galois group G, and let E_1, E_2 be intermediate fields of K which are the splitting fields of irreducible $f_i(x) \in \mathbb{Q}[x]$.

Let $E = E_1E_2 \subset K$.

Let $H_i = \mathrm{Gal}(K/E_i)$ and $H = \mathrm{Gal}(K/E)$.

(a) Show that $H = H_1 \cap H_2$.

(b) Show that H_1H_2 is a subgroup of G.

(c) Show that

$$\mathrm{Gal}(K/(E_1 \cap E_2)) = H_1 H_2.$$

6.4 4.

Let

$$A = \begin{bmatrix} 0 & 1 & -2 \\ 1 & 1 & -3 \\ 1 & 2 & -4 \end{bmatrix} \in M_3(\mathbb{C})$$

(a) Find the Jordan canonical form J of A.

(b) Find an invertible matrix P such that $P^{-1}AP = J$.

You should not need to compute P^{-1}.

6.5 5.

Let

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{and} \quad N = \begin{pmatrix} x & u \\ -y & -v \end{pmatrix}$$

over a commutative ring R, where b and x are units of R. Prove that

$$MN = \begin{pmatrix} 0 & 0 \\ 0 & * \end{pmatrix} \implies MN = 0.$$

6.6 6.

Let

$$M = \{(w, x, y, z) \in \mathbb{Z}^4 \;\big|\; w + x + y + z \in 2\mathbb{Z}\},$$

and

$$N = \{(w, x, y, z) \in \mathbb{Z}^4 \;\big|\; 4 \;\big|\; (w - x),\ 4 \;\big|\; (x - y),\ 4 \;\big|\; (y - z)\}.$$

(a) Show that N is a $\mathbb{Z}$-submodule of M .

(b) Find vectors $u_1, u_2, u_3, u_4 \in \mathbb{Z}^4$ and integers d_1, d_2, d_3, d_4 such that

$$\{u_1, u_2, u_3, u_4\}$$

is a free basis for M, and

$$\{d_1 u_1,\ d_2 u_2,\ d_3 u_3,\ d_4 u_4\}$$

is a free basis for N .

(c) Use the previous part to describe M/N as a direct sum of cyclic $\mathbb{Z}$-modules.

6.7 7.

Let R be a PID and M be an R-module. Let p be a prime element of R. The module M is called $\langle p \rangle$ *-primary* if for every $m \in M$ there exists $k > 0$ such that $p^k m = 0$.

(a) Suppose M is $\langle p \rangle$-primary. Show that if $m \in M$ and $t \in R,\ t \notin \langle p \rangle$, then there exists $a \in R$ such that $atm = m$.

(b) A submodule S of M is said to be *pure* if $S \cap rM = rS$ for all $r \in R$. Show that if M is $\langle p \rangle$-primary, then S is pure if and only if $S \cap p^k M = p^k S$ for all $k \geq 0$.

6.8 8.

Let $R = C[0,1]$ be the ring of continuous real-valued functions on the interval $[0,1]$. Let I be an ideal of R.

(a) Show that if $f \in I, a \in [0,1]$ are such that $f(a) \neq 0$, then there exists $g \in I$ such that $g(x) \geq 0$ for all $x \in [0,1]$, and $g(x) > 0$ for all x in some open neighborhood of a.

(b) If $I \neq R$, show that the set $Z(I) = \left\{x \in [0,1] \;\middle|\; f(x) = 0 \text{ for all } f \in I\right\}$ is nonempty.

(c) Show that if I is maximal, then there exists $x_0 \in [0,1]$ such that $I = \left\{f \in R \;\middle|\; f(x_0) = 0\right\}$.

7 Fall 2017

7.1 1.

Suppose the group G acts on the set A. Assume this action is faithful (recall that this means that the kernel of the homomorphism from G to $\mathrm{Sym}(A)$ which gives the action is trivial) and transitive (for all a, b in A, there exists g in G such that $g \cdot a = b$.)

(a) For $a \in A$, let G_a denote the stabilizer of a in G. Prove that for any $a \in A$,

$$\bigcap_{\sigma \in G} \sigma G_a \sigma^{-1} = \{1\}\,.$$

(b) Suppose that G is abelian. Prove that $|G| = |A|$. Deduce that every abelian transitive subgroup of S_n has order n.

7.2 2.

(a) Classify the abelian groups of order 36.

For the rest of the problem, assume that G is a non-abelian group of order 36.

> You may assume that the only subgroup of order 12 in S_4 is A_4 and that A_4 has no subgroup of order 6.

(b) Prove that if the 2-Sylow subgroup of G is normal, G has a normal subgroup N such that G/N is isomorphic to A_4.

(c) Show that if G has a normal subgroup N such that G/N is isomorphic to A_4 and a subgroup H isomorphic to A_4 it must be the direct product of N and H.

(d) Show that the dihedral group of order 36 is a non-abelian group of order 36 whose Sylow-2 subgroup is not normal.

7.3 3.

Let F be a field. Let $f(x)$ be an irreducible polynomial in $F[x]$ of degree n and let $g(x)$ be any polynomial in $F[x]$. Let $p(x)$ be an irreducible factor (of degree m) of the polynomial $f(g(x))$.

Prove that n divides m. Use this to prove that if r is an integer which is not a perfect square, and n is a positive integer then every irreducible factor of $x^{2n} - r$ over $\mathbb{Q}[x]$ has even degree.

7.4 4.

(a) Let $f(x)$ be an irreducible polynomial of degree 4 in $\mathbb{Q}[x]$ whose splitting field K over $\mathbb{Q}$ has Galois group $G = S_4$.

Let θ be a root of $f(x)$. Prove that $\mathbb{Q}[\theta]$ is an extension of $\mathbb{Q}$ of degree 4 and that there are no intermediate fields between $\mathbb{Q}$ and $\mathbb{Q}[\theta]$.

(b) Prove that if K is a Galois extension of $\mathbb{Q}$ of degree 4, then there is an intermediate subfield between K and $\mathbb{Q}$.

7.5 5.

A ring R is called *simple* if its only two-sided ideals are 0 and R.

(a) Suppose R is a commutative ring with 1. Prove R is simple if and only if R is a field.

(b) Let k be a field. Show the ring $M_n(k)$, $n \times n$ matrices with entries in k, is a simple ring.

7.6 6.

For a ring R, let $U(R)$ denote the multiplicative group of units in R. Recall that in an integral domain R, $r \in R$ is called *irreducible* if r is not a unit in R, and the only divisors of r have the form ru with u a unit in R.

We call a non-zero, non-unit $r \in R$ *prime* in R if $r \mid ab \implies r \mid a$ or $r \mid b$. Consider the ring $R = \{a + b\sqrt{-5} \mid a, b \in Z\}$.

(a) Prove R is an integral domain.

(b) Show $U(R) = \{\pm 1\}$.

(c) Show $3, 2 + \sqrt{-5}$, and $2 - \sqrt{-5}$ are irreducible in R.

(d) Show 3 is not prime in R.

(e) Conclude R is not a PID.

7.7 7.

Let F be a field and let V and W be vector spaces over F .

Make V and W into $F[x]$-modules via linear operators T on V and S on W by defining $X \cdot v = T(v)$ for all $v \in V$ and $X \cdot w = S(w)$ for all w ∈ W .

Denote the resulting $F[x]$-modules by V_T and W_S respectively.

(a) Show that an $F[x]$-module homomorphism from V_T to W_S consists of an F-linear transformation $R : V \longrightarrow W$ such that $RT = SR$.

(b) Show that $VT \cong WS$ as $F[x]$-modules $\iff$ there is an F-linear isomorphism $P : V \longrightarrow W$ such that $T = P^{-1}SP$.

(c) Recall that a module M is *simple* if $M \neq 0$ and any proper submodule of M must be zero. Suppose that V has dimension 2. Give an example of F, T with V_T simple.

(d) Assume F is algebraically closed. Prove that if V has dimension 2, then any V_T is not simple.

8 Spring 2017

8.1 1

Let G be a finite group and $\pi : G \longrightarrow \mathrm{Sym}(G)$ the Cayley representation. (Recall that this means that for an element $x \in G$, $\pi(x)$ acts by left translation on G.)

Prove that $\pi(x)$ is an odd permutation $\iff$ the order $|\pi(x)|$ of $\pi(x)$ is even and $|G|/|\pi(x)|$ is odd.

8.2 2

a. How many isomorphism classes of abelian groups of order 56 are there? Give a representative for one of each class.

b. Prove that if G is a group of order 56, then either the Sylow-2 subgroup or the Sylow-7 subgroup is normal.

c. Give two non-isomorphic groups of order 56 where the Sylow-7 subgroup is normal and the Sylow-2 subgroup is *not* normal. Justify that these two groups are not isomorphic.

8.3 3

Let R be a commutative ring with 1. Suppose that M is a free R-module with a finite basis X.

a. Let $I \trianglelefteq R$ be a proper ideal. Prove that M/IM is a free R/I-module with basis X', where X' is the image of X under the canonical map $M \longrightarrow M/IM$.

b. Prove that any two bases of M have the same number of elements. You may assume that the result is true when R is a field.

8.4 4

a. Let R be an integral domain with quotient field F. Suppose that $p(x), a(x), b(x)$ are monic polynomials in $F[x]$ with $p(x) = a(x)b(x)$ and with $p(x) \in R[x]$, $a(x)$ not in $R[x]$, and both $a(x), b(x)$ not constant. Prove that R is not a UFD. (You may assume Gauss' lemma)

b. Prove that $\mathbb{Z}[2\sqrt{2}]$ is not a UFD.

> Hint: let $p(x) = x^2 - 2$.

8.5 5

Let R be an integral domain and let M be a nonzero torsion R-module.

a. Prove that if M is finitely generated then the annihilator in R of M is nonzero.

b. Give an example of a non-finitely generated torsion R-module whose annihilator is (0), and justify your answer.

8.6 6

Let A be an $n \times n$ matrix with all entries equal to 0 except for the $n-1$ entries just above the diagonal being equal to 2.

a. What is the Jordan canonical form of A, viewed as a matrix in $M_n(\mathbb{C})$?

b. Find a nonzero matrix $P \in M_n(\mathbb{C})$ such that $P^{-1}AP$ is in Jordan canonical form.

8.7 7

Let F be a field and let $f(x) \in F[x]$.

a. Define what a splitting field of $f(x)$ over F is.

b. Let F now be a finite field with q elements. Let E/F be a finite extension of degree $n > 0$. Exhibit an explicit polynomial $g(x) \in F[x]$ such that E/F is a splitting field of $g(x)$ over F. Fully justify your answer.

c. Show that the extension E/F in (b) is a Galois extension.

8.8 8

a. Let K denote the splitting field of $x^5 - 2$ over $\mathbb{Q}$. Show that the Galois group of $K/\mathbb{Q}$ is isomorphic to the group of invertible matrices

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \quad \text{where} \quad a \in \mathbb{F}_5^\times \text{ and } b \in \mathbb{F}_5.$$

b. Determine all intermediate fields between K and $\mathbb{Q}$ which are Galois over $\mathbb{Q}$.

9 Fall 2016

9.1 1

Let G be a finite group and $s, t \in G$ be two distinct elements of order 2. Show that subgroup of G generated by s and t is a dihedral group.

> Recall that the dihedral groups of order $2m$ for $m \geq 2$ are of the form
>
> $$D_{2m} = \left\langle \sigma, \tau \;\middle|\; \sigma^m = 1 = \tau^2, \tau\sigma = \sigma^{-1}\tau \right\rangle.$$

9.2 2

Let A, B be two $n \times n$ matrices with the property that $AB = BA$. Suppose that A and B are diagonalizable. Prove that A and B are *simultaneously* diagonalizable.

9.3 3

How many groups are there up to isomorphism of order pq where $p < q$ are prime integers?

9.4 4

Set $f(x) = x^3 - 5 \in \mathbb{Q}[x]$.

a. Find the splitting field K of $f(x)$ over $\mathbb{Q}$.

b. Find the Galois group G of K over $\mathbb{Q}$.

c. Exhibit explicitly the correspondence between subgroups of G and intermediate fields between $\mathbb{Q}$ and K.

9.5 5

How many monic irreducible polynomials over $\mathbb{F}_p$ of prime degree ℓ are there? Justify your answer.

9.6 6

Let R be a ring and $f : M \longrightarrow N$ and $g : N \longrightarrow M$ be R-module homomorphisms such that $g \circ f = \mathrm{id}_M$. Show that $N \cong \operatorname{im} f \oplus \ker g$.

9.7 7

a. Define what it means for a group G to be *solvable*.

b. Show that every group G of order 36 is solvable.

> Hint: you can use that S_4 is solvable.

9.8 1

10 Spring 2016

10.1 1

Let

$$A = \begin{pmatrix} -3 & 3 & -2 \\ -7 & 6 & -3 \\ 1 & -1 & 2 \end{pmatrix} \in M_3(\mathrm{C}).$$

a. Find the Jordan canonical form J of A.

b. Find an invertible matrix P such that $P^{-1}AP = J$. You do not need to compute P^{-1}.

10.2 2

Let $K = \mathbb{Q}[\sqrt{2} + \sqrt{5}]$.

a. Find $[K : \mathbb{Q}]$.

b. Show that $K/\mathbb{Q}$ is Galois, and find the Galois group G of $K/\mathbb{Q}$.

c. Exhibit explicitly the correspondence between subgroups of G and intermediate fields between $\mathbb{Q}$ and K.

10.3 3

a. State the three Sylow theorems.

b. Prove that any group of order 1225 is abelian.

c. Write down exactly one representative in each isomorphism class of abelian groups of order 1225.

10.4 4

Let R be a ring with the following commutative diagram of R-modules, where each row represents a short exact sequence of R-modules:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} & & \\ 0 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \longrightarrow & 0 \end{array}$$

Prove that if α and γ are isomorphisms then β is an isomorphism.

10.5 5

Let G be a finite group acting on a set X. For $x \in X$, let G_x be the stabilizer of x and $G \cdot x$ be the orbit of x.

a. Prove that there is a bijection between the left cosets G/G_x and $G \cdot x$.

b. Prove that the center of every finite p-group G is nontrivial by considering that action of G on $X = G$ by conjugation.

10.6 6

Let K be a Galois extension of a field F with $[K : F] = 2015$. Prove that K is an extension by radicals of the field F.

10.7 7

Let $D = \mathbb{Q}[x]$ and let M be a $\mathbb{Q}[x]$-module such that

$$M \cong \frac{\mathbb{Q}[x]}{(x-1)^3} \oplus \frac{\mathbb{Q}[x]}{(x^2+1)^3} \oplus \frac{\mathbb{Q}[x]}{(x-1)(x^2+1)^5} \oplus \frac{\mathbb{Q}[x]}{(x+2)(x^2+1)^2}.$$

Determine the elementary divisors and invariant factors of M.

10.8 8

Let R be a simple rng (a nonzero ring which is not assume to have a 1, whose only two-sided ideals are (0) and R) satisfying the following two conditions:

i. R has no zero divisors, and
ii. If $x \in R$ with $x \neq 0$ then $2x \neq 0$, where $2x := x + x$.

Prove the following:

a. For each $x \in R$ there is one and only one element $y \in R$ such that $x = 2y$.
b. Suppose $x, y \in R$ such that $x \neq 0$ and $2(xy) = x$, then $yz = zy$ for all $z \in R$.

> You can get partial credit for (b) by showing it in the case R has a 1.

11 Fall 2015

11.1 1

Let G be a group containing a subgroup H not equal to G of finite index. Prove that G has a normal subgroup which is contained in every conjugate of H which is of finite index.

11.2 2

Let G be a finite group, H a p-subgroup, and P a sylow p-subgroup for p a prime. Let H act on the left cosets of P in G by left translation.

Prove that this is an orbit under this action of length 1.

Prove that xP is an orbit of length 1 $\iff$ H is contained in xPx^{-1}.

11.3 3

Let R be a rng (a ring without 1) which contains an element u such that for all $y \in R$, there exists an $x \in R$ such that $xu = y$.

Prove that R contains a maximal left ideal.

> Hint: imitate the proof (using Zorn's lemma) in the case where R does have a 1.

11.4 4

Let R be a PID and $(a_1) < (a_2) < \cdots$ be an ascending chain of ideals in R. Prove that for some n, we have $(a_j) = (a_n)$ for all $j \geq n$.

11.5 5

Let $u = \sqrt{2+\sqrt{2}}$, $v = \sqrt{2-\sqrt{2}}$, and $E = \mathbb{Q}(u)$.

a. Find (with justification) the minimal polynomial $f(x)$ of u over $\mathbb{Q}$.

b. Show $v \in E$, and show that E is a splitting field of $f(x)$ over $\mathbb{Q}$.

c. Determine the Galois group of E over $\mathbb{Q}$ and determine all of the intermediate fields F such that $\mathbb{Q} \subset F \subset E$.

11.6 6

a. Let G be a finite group. Show that there exists a field extension K/F with $\mathrm{Gal}(K/F) = G$.

> You may assume that for any natural number n there is a field extension with Galois group S_n.

b. Let K be a Galois extension of F with $|\mathrm{Gal}(K/F)| = 12$. Prove that there exists an intermediate field E of K/F with $[E : F] = 3$.

c. With K/F as in (b), does an intermediate field L necessarily exist satisfying $[L : F] = 2$? Give a proof or counterexample.

11.7 7

a. Show that two 3×3 matrices over $\mathbb{C}$ are similar $\iff$ their characteristic polynomials are equal and their minimal polynomials are equal.

b. Does the conclusion in (a) hold for 4×4 matrices? Justify your answer with a proof or counterexample.

11.8 8

Let V be a vector space over a field F and $V^\vee$ its dual. A *symmetric bilinear form* $(\cdot, \cdot)$ on V is a map $V \times V \longrightarrow F$ satisfying

$$(av_1 + bv_2, w) = a(v_1, w) + b(v_2, w) \quad \text{and} \quad (v_1, v_2) = (v_2, v_1)$$

for all $a, b \in F$ and $v_1, v_2 \in V$. The form is *nondegenerate* if the only element $w \in V$ satisfying $(v, w) = 0$ for all $v \in V$ is $w = 0$.

Suppose $(\,\cdot\,,\,\cdot\,)$ is a nondegenerate symmetric bilinear form on V. If W is a subspace of V, define

$$W\perp := \left\{ v \in V \;\middle|\; (v, w) = 0 \text{ for all } w \in W \right\}.$$

a. Show that if X, Y are subspaces of V with $Y \subset X$, then $X\perp \subseteq Y\perp$.

b. Define an injective linear map

$$\psi : Y\perp / X\perp \hookrightarrow (X/Y)^\vee$$

which is an isomorphism if V is finite dimensional.

12 Spring 2015 ("Winter 2015")

12.1 1

For a prime p, let G be a finite p-group and let N be a normal subgroup of G of order p. Prove that N is contained in the center of G.

12.2 2

Let $\mathbb{F}$ be a finite field.

a. Give (with proof) the decomposition of the additive group $(\mathbb{F}, +)$ into a direct sum of cyclic groups.

b. The *exponent* of a finite group is the least common multiple of the orders of its elements. Prove that a finite abelian group has an element of order equal to its exponent.

c. Prove that the multiplicative group $(\mathbb{F}^\times, \cdot)$ is cyclic.

12.3 3

Let F be a field and V a finite dimensional F-vector space, and let $A, B : V \longrightarrow V$ be commuting F-linear maps. Suppose there is a basis $\mathcal{B}_1$ with respect to which A is diagonalizable and a basis $\mathcal{B}_2$ with respect to which B is diagonalizable.

Prove that there is a basis $\mathcal{B}_3$ with respect to which A and B are both diagonalizable.

12.4 4

Let N be a positive integer, and let G be a finite group of order N.

a. Let $\mathrm{Sym}G$ be the set of all bijections from $G \longrightarrow G$ viewed as a group under composition. Note that $\mathrm{Sym}G \cong S_N$. Prove that the Cayley map

$$\begin{aligned} C : G &\longrightarrow \mathrm{Sym}G \\ g &\mapsto (x \mapsto gx) \end{aligned}$$

is an injective homomorphism.

b. Let $\Phi : \mathrm{Sym}G \longrightarrow S_N$ be an isomorphism. For $a \in G$ define $\varepsilon(a) \in \{\pm 1\}$ to be the sign of the permutation $\Phi(C(a))$. Suppose that a has order d. Prove that $\varepsilon(a) = -1 \iff d$ is even and N/d is odd.

c. Suppose $N > 2$ and $n \equiv 2 \mod 4$. Prove that G is not simple.

Hint: use part (b).

12.5 5

Let $f(x) = x^4 - 5 \in \mathbb{Q}[x]$.

a. Compute the Galois group of f over $\mathbb{Q}$.
b. Compute the Galois group of f over $\mathbb{Q}(\sqrt{5})$.

12.6 6

Let F be a field and n a positive integer, and consider

$$A = \begin{bmatrix} 1 & \dots & 1 \\ & \ddots & \\ 1 & \dots & 1 \end{bmatrix} \in M_n(F).$$

Show that A has a Jordan normal form over F and find it.

Hint: treat the cases $n \cdot 1 \neq 0$ in F and $n \cdot 1 = 0$ in F separately.

12.7 7

Let R be a commutative ring, and $S \subset R$ be a nonempty subset that does not contain 0 such that for all $x, y \in S$ we have $xy \in S$. Let $\mathcal{I}$ be the set of all ideals $I \trianglelefteq R$ such that $I \bigcap S = \emptyset$.

Show that for every ideal $I \in \mathcal{I}$, there is an ideal $J \in \mathcal{I}$ such that $I \subset J$ and J is not properly contained in any other ideal in $\mathcal{I}$.

Prove that every such ideal J is prime.

12.8 8

Let R be a PID and M a finitely generated R-module.

a. Prove that there are R-submodules

$$0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$$

such that for all $0 \leq i \leq n-1$, the module M_{i+1}/M_i is cyclic.

b. Is the integer n in part (a) uniquely determined by M? Prove your answer.

13 Fall 2014

13.1 1

Let $f \in \mathbb{Q}[x]$ be an irreducible polynomial and L a finite Galois extension of $\mathbb{Q}$. Let $f(x) = g_1(x)g_2(x)\cdots g_r(x)$ be a factorization of f into irreducibles in $L[x]$.

a. Prove that each of the factors $g_i(x)$ has the same degree.

b. Give an example showing that if L is not Galois over $\mathbb{Q}$, the conclusion of part (a) need not hold.

13.2 2

Let G be a group of order 96.

a. Show that G has either one or three 2-Sylow subgroups.

b. Show that either G has a normal subgroup of order 32, or a normal subgroup of order 16.

13.3 3

Consider the polynomial $f(x) = x^4 - 7 \in \mathbb{Q}[x]$ and let $E/\mathbb{Q}$ be the splitting field of f.

a. What is the structure of the Galois group of $E/\mathbb{Q}$?

b. Give an explicit description of all of the intermediate subfields $\mathbb{Q} \subset K \subset E$ in the form $K = \mathbb{Q}(\alpha), \mathbb{Q}(\alpha, \beta), \cdots$ where α, β, etc are complex numbers. Describe the corresponding subgroups of the Galois group.

13.4 4

Let F be a field and T an $n \times n$ matrix with entries in F. Let I be the ideal consisting of all polynomials $f \in F[x]$ such that $f(T) = 0$.

Show that the following statements are equivalent about a polynomial $g \in I$:

a. g is irreducible.

b. If $k \in F[x]$ is nonzero and of degree strictly less than g, then $k[T]$ is an invertible matrix.

13.5 5

Let T be a 5×5 complex matrix with characteristic polynomial $\chi(x) = (x-3)^5$ and minimal polynomial $m(x) = (x-3)^2$. Determine all possible Jordan forms of T.

13.6 6

Let G be a group and $H, K < G$ be subgroups of finite index. Show that

$$[G : H \bigcap K] \leq [G : H]\ [G : K].$$

13.7 7

Give a careful proof that $\mathbb{C}[x, y]$ is not a PID.

13.8 8

Let R be a nonzero commutative ring without unit such that R does not contain a proper maximal ideal. Prove that for all $x \in R$, the ideal xR is proper. You may assume the axiom of choice.

14 Spring 2014

14.1 1

Let p, n be integers such that p is prime and p does not divide n. Find a real number $k = k(p, n)$ such that for every integer $m \geq k$, every group of order $p^m n$ is not simple.

14.2 2

Let $G \subset S_9$ be a Sylow-3 subgroup of the symmetric group on 9 letters.

a. Show that G contains a subgroup H isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ by exhibiting an appropriate set of cycles.

b. Show that H is normal in G.

c. Give generators and relations for G as an abstract group, such that all generators have order 3. Also exhibit elements of S_9 in cycle notation corresponding to these generators.

d. Without appealing to the previous parts of the problem, show that G contains an element of order 9.

14.3 3

Let $F \subset C$ be a field extension with C algebraically closed.

a. Prove that the intermediate field $C_{\text{alg}} \subset C$ consisting of elements algebraic over F is algebraically closed.

b. Prove that if $F \longrightarrow E$ is an algebraic extension, there exists a homomorphism $E \longrightarrow C$ that is the identity on F.

14.4 4

Let $E \subset \mathbb{C}$ denote the splitting field over $\mathbb{Q}$ of the polynomial $x^3 - 11$.

a. Prove that if n is a squarefree positive integer, then $\sqrt{n} \notin E$.

> Hint: you can describe all quadratic extensions of $\mathbb{Q}$ contained in E.

b. Find the Galois group of $(x^3 - 11)(x^2 - 2)$ over $\mathbb{Q}$.

c. Prove that the minimal polynomial of $11^{1/3} + 2^{1/2}$ over $\mathbb{Q}$ has degree 6.

14.5 5

Let R be a commutative ring and $a \in R$. Prove that a is not nilpotent $\iff$ there exists a commutative ring S and a ring homomorphism $\varphi : R \longrightarrow S$ such that $\varphi(a)$ is a unit.

Note: by definition, a is nilpotent $\iff$ there is a natural number n such that $a^n = 0$.

14.6 6

Let R be a commutative ring with identity and let n be a positive integer.

a. Prove that every surjective R-linear endomorphism $T : R^n \longrightarrow R^n$ is injective.

b. Show that an injective R-linear endomorphism of R^n need not be surjective.

14.7 7

Let $G = \mathrm{GL}(3, \mathbb{Q}[x])$ be the group of invertible 3×3 matrices over $\mathbb{Q}[x]$. For each $f \in \mathbb{Q}[x]$, let S_f be the set of 3×3 matrices A over $\mathbb{Q}[x]$ such that $\det(A) = cf(x)$ for some nonzero constant $c \in \mathbb{Q}$.

a. Show that for $(P, Q) \in G \times G$ and $A \in S_f$, the formula

$$(P, Q) \cdot A \coloneqq PAQ^{-1}$$

gives a well defined map $G \times G \times S_f \longrightarrow S_f$ and show that this map gives a group action of $G \times G$ on S_f.

b. For $f(x) = x^3(x^2 + 1)^2$, give one representative from each orbit of the group action in (a), and justify your assertion.

15 Fall 2013

15.1 1

Let p, q be distinct primes.

a. Let $\bar{q} \in \mathbb{Z}_p$ be the class of $q \mod p$ and let k denote the order of $\bar{q}$ as an element of $\mathbb{Z}_p^{\times}$. Prove that no group of order pq^k is simple.

b. Let G be a group of order pq, and prove that G is not simple.

15.2 2

Let G be a group of order 30.

a. Show that G has a subgroup of order 15.

b. Show that every group of order 15 is cyclic.

c. Show that G is isomorphic to some semidirect product $\mathbb{Z}_{15} \rtimes \mathbb{Z}_2$.

d. Exhibit three nonisomorphic groups of order 30 and prove that they are not isomorphic. You are not required to use your answer to (c).

15.3 3

a. Define *prime ideal*, give an example of a nontrivial ideal in the ring $\mathbb{Z}$ that is not prime, and prove that it is not prime.

b. Define *maximal ideal*, give an example of a nontrivial maximal ideal in $\mathbb{Z}$ and prove that it is maximal.

15.4 4

Let R be a commutative ring with $1 \neq 0$. Recall that $x \in R$ is *nilpotent* iff $x^n = 0$ for some positive integer n.

a. Show that the collection of nilpotent elements in R forms an ideal.

b. Show that if x is nilpotent, then x is contained in every prime ideal of R.

c. Suppose $x \in R$ is not nilpotent and let $S = \left\{ x^n \;\middle|\; n \in \mathbb{N} \right\}$. There is at least on ideal of R disjoint from S, namely (0). By Zorn's lemma the set of ideals disjoint from S has a maximal element with respect to inclusion, say I. In other words, I is disjoint from S and if J is any ideal disjoint from S with $I \subseteq J \subseteq R$ then $J = I$ or $J = R$.

Show that I is a prime ideal.

d. Deduce from (a) and (b) that the set of nilpotent elements of R is the intersection of all prime ideals of R.

15.5 5

Let L/K be a finite extension of fields.

a. Define what it means for L/K to be *separable*.

b. Show that if K is a finite field, then L/K is always separable.

c. Give an example of a finite extension L/K that is not separable.

15.6 6

Let K be the splitting field of $x^4 - 2$ over $\mathbb{Q}$ and set $G = \mathrm{Gal}(K/\mathbb{Q})$.

a. Show that $K/\mathbb{Q}$ contains both $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt[4]{2})$ and has degree 8 over $\mathbb{Q}$/

b. Let $N = \mathrm{Gal}(K/\mathbb{Q}(i))$ and $H = \mathrm{Gal}(K/\mathbb{Q}(\sqrt[4]{2}))$. Show that N is normal in G and $NH = G$.

Hint: what field is fixed by NH?

c. Show that $\mathrm{Gal}(K/\mathbb{Q})$ is generated by elements σ, τ, of orders 4 and 2 respectively, with $\tau\sigma\tau^{-1} = \sigma^{-1}$.

Equivalently, show it is the dihedral group of order 8.

d. How many distinct quartic subfields of K are there? Justify your answer.

15.7 7

Let $F = \mathbb{F}_2$ and let $\overline{F}$ denote its algebraic closure.

a. Show that $\overline{F}$ is not a finite extension of F.

b. Suppose that $\alpha \in \overline{F}$ satisfies $\alpha^{17} = 1$ and $\alpha \neq 1$. Show that $F(\alpha)/F$ has degree 8.

16 Spring 2013

16.1 1

Let R be a commutative ring.

a. Define a *maximal ideal* and prove that R has a maximal ideal.

b. Show than an element $r \in R$ is not invertible $\iff$ r is contained in a maximal ideal.

c. Let M be an R-module, and recall that for $0 \neq \mu \in M$, the *annihilator* of μ is the set

$$\operatorname{Ann}(\mu) = \left\{ r \in R \;\middle|\; r\mu = 0 \right\}.$$

Suppose that I is an ideal in R which is maximal with respect to the property that there exists an element $\mu \in M$ such that $I = \operatorname{Ann}(\mu)$ for some $\mu \in M$. In other words, $I = \operatorname{Ann}(\mu)$ but there does not exist $\nu \in M$ with $J = \operatorname{Ann}(\nu) \subsetneq R$ such that $I \subsetneq J$.

Prove that I is a prime ideal.

16.2 2

a. Define a *Euclidean domain*.

b. Define a *unique factorization domain*.

c. Is a Euclidean domain an UFD? Give either a proof or a counterexample with justification.

d. Is a UFD a Euclidean domain? Give either a proof or a counterexample with justification.

16.3 3

Let P be a finite p-group. Prove that every nontrivial normal subgroup of P intersects the center of P nontrivially.

16.4 4

Define a *simple group*. Prove that a group of order 56 can not be simple.

16.5 5

Let $T : V \longrightarrow V$ be a linear map from a 5-dimensional $\mathbb{C}$-vector space to itself and suppose $f(T) = 0$ where $f(x) = x^2 + 2x + 1$.

a. Show that there does not exist any vector $v \in V$ such that $Tv = v$, but there *does* exist a vector $w \in V$ such that $T^2 w = w$.

b. Give all of the possible Jordan canonical forms of T.

16.6 6

Let V be a finite dimensional vector space over a field F and let $T : V \longrightarrow V$ be a linear operator with characteristic polynomial $f(x) \in F[x]$.

a. Show that $f(x)$ is irreducible in $F[x] \iff$ there are no proper nonzero subspaces $W < V$ with $T(W) \subseteq W$.

b. If $f(x)$ is irreducible in $F[x]$ and the characteristic of F is 0, show that T is diagonalizable when we extend the field to its algebraic closure.

16.7 7

Let $f(x) = g(x)h(x) \in \mathbb{Q}[x]$ and $E, B, C/\mathbb{Q}$ be the splitting fields of f, g, h respectively.

a. Prove that $\mathrm{Gal}(E/B)$ and $\mathrm{Gal}(E/C)$ are normal subgroups of $\mathrm{Gal}(E/\mathbb{Q})$.

b. Prove that $\mathrm{Gal}(E/B) \bigcap \mathrm{Gal}(E/C) = \{1\}$.

c. If $B \bigcap C = \mathbb{Q}$, show that $\mathrm{Gal}(E/B)\mathrm{Gal}(E/C) = \mathrm{Gal}(E/\mathbb{Q})$.

d. Under the hypothesis of (c), show that $\mathrm{Gal}(E/\mathbb{Q}) \cong \mathrm{Gal}(E/B) \times \mathrm{Gal}(E/C)$.

e. Use (d) to describe $\mathrm{Gal}(\mathbb{Q}[\alpha]/\mathbb{Q})$ where $\alpha = \sqrt{2} + \sqrt{3}$.

16.8 8

Let F be the field with 2 elements and K a splitting field of $f(x) = x^6 + x^3 + 1$ over F. You may assume that f is irreducible over F.

a. Show that if r is a root of f in K, then $r^9 = 1$ but $r^3 \neq 1$.

b. Find $\mathrm{Gal}(K/F)$ and express each intermediate field between F and K as $F(\beta)$ for an appropriate $\beta \in K$.

17 Fall 2012

17.1 1

Let G be a finite group and X a set on which G acts.

a. Let $x \in X$ and $G_x \coloneqq \left\{ g \in G \,\middle|\, g \cdot x = x \right\}$. Show that G_x is a subgroup of G.

b. Let $x \in X$ and $G \cdot x \coloneqq \left\{ g \cdot x \,\middle|\, g \in G \right\}$. Prove that there is a bijection between elements in $G \cdot x$ and the left cosets of G_x in G.

17.2 2

Let G be a group of order 30.

a. Show that G contains normal subgroups of orders 3, 5, and 15.

b. Give all possible presentations and relations for G.

c. Determine how many groups of order 30 there are up to isomorphism.

17.3 3

Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree 5. Assume that f has all but two roots in $\mathbb{R}$. Compute the Galois group of $f(x)$ over $\mathbb{Q}$ and justify your answer.

17.4 4

Let $f(x) \in \mathbb{Q}[x]$ be a polynomial and K be a splitting field of f over $\mathbb{Q}$. Assume that $[K : \mathbb{Q}] = 1225$ and show that $f(x)$ is solvable by radicals.

17.5 5

Let U be an infinite-dimensional vector space over a field k, $f : U \longrightarrow U$ a linear map, and $\{u_1, \cdots, u_m\} \subset U$ vectors such that U is generated by $\left\{u_1, \cdots, u_m, f^d(u_1), \cdots, f^d(u_m)\right\}$ for some $d \in \mathbb{N}$.

Prove that U can be written as a direct sum $U \cong V \oplus W$ such that

1. V has a basis consisting of some vector $v_1, \cdots v_n, f^d(v_1), \cdots, f^d(v_n)$ for some $d \in \mathbb{N}$, and
2. W is finite-dimensional.

Moreover, prove that for any other decomposition $U \cong V' \oplus W'$, one has $W' \cong W$.

17.6 6

Let R be a ring and M an R-module. Recall that M is *Noetherian* iff any strictly increasing chain of submodule $M_1 \subsetneq M_2 \subsetneq \cdots$ is finite. Call a proper submodule $M' \subsetneq M$ *intersection-decomposable* if it can not be written as the intersection of two proper submodules $M' = M_1 \bigcap M_2$ with $M_i \subsetneq M$.

Prove that for every Noetherian module M, any proper submodule $N \subsetneq M$ can be written as a finite intersection $N = N_1 \bigcap \cdots \bigcap N_k$ of intersection-indecomposable modules.

17.7 7

Let k be a field of characteristic zero and $A, B \in M_n(k)$ be two square $n \times n$ matrices over k such that $AB - BA = A$. Prove that $\det A = 0$.

Moreover, when the characteristic of k is 2, find a counterexample to this statement.

17.8 8

Prove that any nondegenerate matrix $X \in M_n(\mathbb{R})$ can be written as $X = UT$ where U is orthogonal and T is upper triangular.

18 Spring 2012

18.1 1

Suppose that $F \subset E$ are fields such that E/F is Galois and $|\mathrm{Gal}(E/F)| = 14$.

a. Show that there exists a unique intermediate field K with $F \subset K \subset E$ such that $[K : F] = 2$.

b. Assume that there are at least two distinct intermediate subfields $F \subset L_1, L_2 \subset E$ with $[L_i : F] = 7$. Prove that $\mathrm{Gal}(E/F)$ is nonabelian.

18.2 2

Let G be a finite group and p a prime number such that there is a normal subgroup $H \trianglelefteq G$ with $|H| = p^i > 1$.

a. Show that H is a subgroup of any Sylow p-subgroup of G.

b. Show that G contains a nonzero abelian normal subgroup of order divisible by p.

18.3 3

Let G be a group of order 70.

a. Show that G is not simple.

b. Exhibit 3 nonisomorphic groups of order 70 and prove that they are not isomorphic.

18.4 4

Let $f(x) = x^7 - 3 \in \mathbb{Q}[x]$ and $E/\mathbb{Q}$ be a splitting field of f with $\alpha \in E$ a root of f.

a. Show that E contains a primitive 7th root of unity.

b. Show that $E \neq \mathbb{Q}(\alpha)$.

18.5 5

Let M be a finitely generated module over a PID R.

a. M_t be the set of torsion elements of M, and show that M_t is a submodule of M.

b. Show that M/M_t is torsion free.

c. Prove that $M \cong M_t \oplus F$ where F is a free module.

18.6 6

Let k be a field and let the group $G = \mathrm{GL}(m,k) \times \mathrm{GL}(n,k)$ acts on the set of $m \times n$ matrices $M_{m,n}(k)$ as follows:

$$(A,B) \cdot X = AXB^{-1}$$

where $(A,B) \in G$ and $X \in M_{m,n}(k)$.

a. State what it means for a group to act on a set. Prove that the above definition yields a group action.

b. Exhibit with justification a subset S of $M_{m,n}(k)$ which contains precisely one element of each orbit under this action.

18.7 7

Consider the following matrix as a linear transformation from $V \coloneqq \mathbb{C}^5$ to itself:

$$A = \begin{pmatrix} -1 & 1 & 0 & 0 & 0 \\ -4 & 3 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 2 \end{pmatrix}.$$

a. Find the invariant factors of A.

b. Express V in terms of a direct sum of indecomposable $\mathbb{C}[x]$-modules.

c. Find the Jordan canonical form of A.

18.8 8

Let V be a finite-dimensional vector space over a field k and $T : V \longrightarrow V$ a linear transformation.

a. Provide a definition for the *minimal polynomial* in $k[x]$ for T.

b. Define the *characteristic polynomial* for T.

c. Prove the Cayley-Hamilton theorem: the linear transformation T satisfies its characteristic polynomial.