# UGA Algebra Qualifying Exam Questions

D. Zack Garza

Monday 8th June, 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 $\alpha^{2020}$ 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 $N \cong \mathrm{im}\, f \oplus \ker g$.

## 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 torsion 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 Spring 2019

### 2.1 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 $\mathbb{C}$.

### 2.2 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 $n$.

### 2.3 3.

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

Describe a representative from each class.

### 2.4 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 $G$.

### 2.5 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.

### 2.6 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.

### 2.7 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.

### 2.8 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 $\mathbb{Q}$?

# 3 Fall 2019

## 3.1 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.

## 3.2 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.

## 3.3 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.

## 3.4 4

Let $F$ be a finite field with $q$ elements.

Let $n$ be a positive integer relatively prime to $q$ and let $\omega$ be a primitive $n$th 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 $m = k$.

## 3.5 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.

## 3.6 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.

## 3.7 7

Let $\zeta_n$ denote a primitive $n$th root of $1 \in \mathbb{Q}$. You may assume the roots of the minimal polynomial $p_n(x)$ of $\zeta_n$ are exactly the primitive $n$th 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 $\mathbb{Q}(\zeta_{20})$?

## 3.8 8

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

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

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 $\Lambda$ to be

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

(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 $\det M = |\Lambda^\vee/\Lambda|$.

# 4 2019 Course Exams

## 4.1 Midterm

1. Let $G$ be a group of order $p^2q$ 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 $\tau$ is a transposition and $\sigma$ 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 $\zeta_n$ be a primitive $n$th root of unity. Show that $[\mathbb{Q}(\zeta_n + \zeta_n^{-1}) : \mathbb{Q}] = \varphi(n)/2$ for $\varphi$ 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 $[L : K]$.

## 4.2 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

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

   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.

# 5 Spring 2018

## 5.1 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 $5^2 \cdot 7^2$.

## 5.2 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 $k$.

## 5.3 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

$$\mathrm{Gal}(K/(E_1 \cap E_2)) = H_1H_2.$$

## 5.4 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 $P^{-1}$.

## 5.5 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

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

## 5.6 6.

Let

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

and

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

(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

$$\{d_1u_1,\ d_2u_2,\ d_3u_3,\ d_4u_4\}$$

is a free basis for $N$ .

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

### 5.7 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 $k \geq 0$.

### 5.8 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 $Z(I) = \{x \in [0,1] \;\middle|\; f(x) = 0 \text{ for all } f \in I\}$ is nonempty.

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

## 6 Fall 2018

### 6.1 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 $b \leq c$.

### 6.2 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 $S$.

### 6.3 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 $L/F$.

### 6.4 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 $\varphi$-invariant subspaces of $V$ , $\varphi|_U$ is nilpotent, and $\varphi|_W$ is nonsingular.

### 6.5 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.

### 6.6 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 $M$.

### 6.7 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:
>
> $$\frac{\mathbb{Z}}{4\mathbb{Z}}, \quad \frac{\frac{\mathbb{Z}}{2\mathbb{Z}}[t]}{(t^2+t+1)}, \quad \frac{\frac{\mathbb{Z}}{2\mathbb{Z}}[t]}{(t^2-t)}, \quad \frac{\frac{\mathbb{Z}}{2\mathbb{Z}}[t]}{(t^2)}.$$

# 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 $\theta$ 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.