ALGEBRA QUALIFYING EXAMS

Herein are solutions to many of the problems on old qualifying exams. Sometimes multiple solutions are given. Some solutions were written years ago when I knew much less (that may make the solutions better or worse, depending on your point of view—but it also might mean that the solutions are incorrect). Comments to myself appear in brackets, whose presence further indicates that you're peeking at a preliminary draft of something. Although I sometimes obtained solutions from listening to others or reading their work (and I try to give credit wherever this is the case), I typed up the solutions myself using style according to my whim and taste (or lack thereof); hence if anyone is to be blamed for incorrect solutions, typos, style, and such, it is I, me, myself, I, and no one else.

I would appreciate your help with this document; if you have solutions to unsolved problems or have corrections or comments on material that appears here, please let me know. Thanks.

SAMPLE PROBLEMS FROM LOUISIANA STATE UNIVERSITY

1. Let $\phi\colon G_1 \to G_2$ be a group homomorphism. Define "kernel of ϕ" and prove that the kernel of ϕ is a normal subgroup of G_1.

SOLUTION:

The **kernel** of ϕ is the set of elements of G_1 that are mapped to the identity element of G_2 by the homomorphism ϕ; in symbols, $\mathrm{KER}(\phi) = \{ g \in G_1 : \phi(g) = 1_{G_2} \}$, where 1_{G_2} denotes the identity element of G_2. To show that $\mathrm{KER}(\phi)$ is a normal subgroup of G_1, I must show the following:

- $\mathrm{KER}(\phi)$ is nonempty;

- Whenever $g, h \in \mathrm{Ker}(\phi)$, also $gh^{-1} \in \mathrm{Ker}(\phi)$;
- $\mathrm{Ker}(\phi)$ is fixed (as a set, not pointwise) under conjugation by any element of G_1, i.e., $G_1 \mathrm{Ker}(\phi) = \mathrm{Ker}(\phi) G_1$.

The first two items show $\mathrm{Ker}(\phi)$ to be a subgroup; the last item shows it to be normal. Since group homomorphisms take the identity to the identity, we have $1_{G_1} \in \mathrm{Ker}(\phi)$, showing $\mathrm{Ker}(\phi)$ to be nonempty. Let $g, h \in \mathrm{Ker}(\phi)$, i.e., $\phi(g) = \phi(h) = 1_{G_2}$. Then $\phi(gh^{-1}) = \phi(g)\phi(h)^{-1} = 1_{G_2} 1_{G_2}^{-1} = 1_{G_2} 1_{G_2} = 1_{G_2}$, and I conclude $gh^{-1} \in \mathrm{Ker}(\phi)$, so that we now know that $\mathrm{Ker}(\phi)$ is a subgroup. Finally, fix arbitrary elements $g \in G_1$ and $k \in \mathrm{Ker}(\phi)$. I claim that the conjugated element gkg^{-1} also lies in $\mathrm{Ker}(\phi)$; indeed, I have $\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g)^{-1} = \phi(g)\, 1_{G_2}\, \phi(g)^{-1} = \phi(g)\phi(g)^{-1} = 1_{G_2}$. This completes the proof that $\mathrm{Ker}(\phi)$ is a normal subgroup of G_1.

---

2. Prove that every group of order 15 is abelian.

SOLUTION:

Certainly groups of order 15 exist—for any order, there is always at least the cyclic group. So fix G to be an arbitrary group of order 15. The 3-Sylow subgroups of G have order 3 and the number of them is congruent to 1 modulo 3 and divides 5; hence there is a single 3-Sylow subgroup, call it H. Note that $H \cong \mathbb{Z}/3\mathbb{Z}$ and furthermore, since the Sylow subgroups of a particular order form an orbit under conjugation, H must be normal in G. The 5-Sylow subgroups of G have order 5 and the number of them is congruent to 1 modulo 5 and divides 3; hence there is a single 5-Sylow subgroup, call it K. As before, we have $K \cong \mathbb{Z}/5\mathbb{Z}$, and K is normal in G. I shall now show that G is the internal direct sum of H and K. The order of any element common to both H and K must simultaneously divide 3 and 5; thus, $H \cap K = \{1\}$. Whenever two normal subgroups meet only in the identity and the product of their orders gives the order of the full group, then the full group is the internal direct sum of these subgroups. Hence $G = H \oplus K \cong (\mathbb{Z}/3\mathbb{Z}) \oplus (\mathbb{Z}/5\mathbb{Z})$, an abelian group.

---

3. Define "solvable group" and prove that a subgroup of a solvable group is solvable.

SOLUTION:

I shall give two definitions for a group to be solvable:

- A group G is **solvable** if the subgroup series $G \geq G' \geq G'' \geq \cdots$ is finite and ends in the trivial subgroup. (Here $G' = [G, G]$ denotes the commutator subgroup of G, also called the derived group, which is the normal subgroup generated by all commutators $[g, h] = g^{-1}h^{-1}gh$.)
- A group G is **solvable** if G possesses a "finite subnormal series with abelian quotients", i.e., there exists a subgroup series $G = H_1 \geq H_2 \geq \cdots \geq H_n = \{1\}$, finite and ending in the trivial subgroup, with the important properties that each subgroup in the series is normal in the previous subgroup, and each quotient H_k/H_{k+1} of neighboring subgroups is abelian.

These definitions turn out to be equivalent. (They had better be, or they couldn't compete for defining the same adjective.) Note that a finite derived series $G \geq G' \geq G'' \geq \cdots \geq \{1\}$ already is a finite subnormal series with abelian quotients. In establishing the equivalency of the two definitions of solvable, the hard direction is showing that the existence of a finite subnormal series with abelian quotients forces the derived series to end in the trivial subgroup after a finite number of steps.

Let $H \leq G$ be a subgroup. Any commutator in H is also a commutator in G, i.e., $H' \leq G'$. Repeating the argument, we get $H'' \leq G''$, $H''' \leq G'''$, and so on. Hence, if G has a finite derived series $G \geq G' \geq G'' \geq \cdots \geq \{1\}$, then the derived series of H must also end in the trivial subgroup and can be no longer than that of G. In other words, the solvability of G implies the solvability of H.

QUESTIONS: [Incorporate with answers into another problem or into separate notes on group theory.]

- Are there interesting examples of solvable groups for which the derived series is the only finite subnormal series with abelian quotients? If so, I would argue that the finite derived series should be *the* definition of solvable, with the separate theorem noting that if one can show the existence of any finite subnormal series with abelian quotients, then one has a finite derived series. The point is that there seems to be little use in working with an abstract finite subnormal series with abelian quotients to conclude something about a group, when one may always take a particular such series, namely the derived series, and in many cases is forced to be working with the derived series. (Working with the abstract series may convince one that one is not using properties specific to the derived series, but I'm not convinced there is much to be gained from this abstraction.)

- How does one easily show the equivalency of the two definitions?
- I should show, given a short exact sequence $1 \to H \to G \to K \to 1$, that solvability of the middle is equivalent to solvability of the two outsides. Are there any other basic properties of solvability that should be established so that the concept may be easily manipulated with diagrams and such?

NOTES: [The following might form the beginning of my notes on normal series, composition series, etc.]

Here follow the basic definitions for normal series and composition series of groups. The main named theorem, the Jordan–Hölder theorem, is now viewed as a simple consequence of Otto Schreier's fundamental theorem on normal series. [Basically copy the exposition in van der Waerden, except be clearer on the idea of when a group does or does not possess a composition series, in particular what are the possibilities for finite groups? Probably any edition is okay, but I liked the information in the revised English edition, 1953, translated from second revised German eidition by Fred Blum.]

---

4. Prove that if the polynomials $f(x)$ and $g(x)$ are relatively prime in the polynomial ring $K[x]$, where K denotes a field, then

$$\big(f(x)\big) + \big(g(x)\big) = K[x].$$

SOLUTION:

By definition, $f(x)$ and $g(x)$ being relatively prime means that their greatest common divisor may be taken to be 1, i.e., any common divisor must be a unit. Since $K[x]$ is a principal ideal domain, the smallest ideal containing both $f(x)$ and $g(x)$ is the ideal generated by the GCD of these elements, so in this problem that would be the entire ring. In case my solution is quoting too many facts, let me explain some more. In a principal ideal domain, the GCD of two elements is expressible as a combination of the two elements: $1 = a(x)f(x) + b(x)g(x)$. In fact, since $K[x]$ is furthermore a Euclidean domain, there is an algorithm for computing $a(x)$ and $b(x)$. Now $a(x)f(x) \in \big(f(x)\big)$ and $b(x)g(x) \in \big(g(x)\big)$; thus their sum, the unit 1, lies in $\big(f(x)\big) + \big(g(x)\big)$, showing the latter to be the entire ring $K[x]$.

---

5. Prove that if the subgroup B has index 2 in the group A, then B is normal in A.

SOLUTION:

The group A is partitioned by the left cosets of B, and A is also partitioned by the right cosets of B. One characterization of normality is the following: the subgroup B is normal if and only if the two partitions are identical. (This characterization is merely a restating in words of the definition of normality: $Bx = xB$ for all $x \in A$.)

In the present situation, B has index 2. Thus there are precisely two left cosets and precisely two right cosets. Since the identity left coset always equals the identity right coset, the remaining cosets, being simply what remains, must also be equal. Put another way, the following statements are equivalent for an element $x \in A$:

- x is in some nonidentity left coset;
- x is not in the identity left coset;
- x is not in the identity right coset;
- x is in some nonidentity right coset.

Incidentally, the argument above is valid for infinite groups; for finite groups, the above result is a special case of the following general result: if the index of a subgroup is the smallest prime dividing the order of the full group, then the subgroup is normal. But the proof is more difficult.

Let $H \leq G$ with $|G/H| = p$. Let G act on the left cosets of H by left translation. Thus we get a homomorphism $G \to S_p$ whose kernel is at least H. If the kernel were any larger, it would be all of G (since its index could only be 1), but the kernel must be proper since the image of the homomorphism is a transitive subgroup of S_p (this action is transitive). Hence the kernel is precisely H, and thus H is normal.

[Perhaps following is a different proof: the subgroup of smallest prime index must be a maximal proper subgroup. Can one show that they are characteristic? That would be stronger than normal.]

---

6. Find the commutator subgroup of the symmetric group S_3.

SOLUTION:

The commutator subgroup of any group is the subgroup generated by all commutators (and usually comprises more than just the commutators). It happens to be a normal subgroup and is the smallest normal subgroup such that the quotient group is abelian. Since S_3 is not abelian, the commutator subgroup is not trivial; the only proper nontrivial normal subgroup of S_3 is the cyclic subgroup of order 3 generated by (123); since the quotient group is cyclic of order 2 and thus abelian, the subgroup generated by (123) must be the commutator subgroup.

---

7. Give an example of two nonzero abelian groups A and B such that the set $\mathrm{Hom}(A, B)$ of all group homomorphisms equals 0.

SOLUTION:

Let $A = \mathbb{Z}/2\mathbb{Z}$ and $B = \mathbb{Z}/3\mathbb{Z}$. (That is, let A, B be the additive groups of the indicated rings.) Let $\phi\colon A \to B$ be a homomorphism. We know $\phi(0) = 0$, and thus $0 = \phi(0) = \phi(1+1) = \phi(1) + \phi(1)$; we see that $\phi(1)$ is an element in B with the property that adding it to itself gives 0. But $1 + 1 = 2$ and $2 + 2 = 1$; thus, we must have $\phi(1) = 0$. Thus the arbitrary homomorphism ϕ sends all elements of A to 0; we conclude $\mathrm{Hom}(A, B) = 0$.

---

8. Let F be a finite field with exactly q elements. What can you say about q? Explain briefly how to construct a finite field with exactly 4 elements. Can a field with 27 elements contain a field with 9 elements? Explain.

SOLUTION:

If F is a finite field with q elements, then $q = p^m$ for some prime number p and some integer $m \geq 1$. To construct a field with 4 elements, take the field $F = \mathbb{Z}/2\mathbb{Z}$ and consider $F[x]/(x^2 + x + 1)$; its elements are the cosets represented by 0, 1, x, and $1 + x$. A field with 27 elements certainly contains a subfield with 3 elements, but it cannot contain a subfield with 9 elements; if it did, it would be an extension of degree ≥ 2 over the subfield, and that puts at least 81 elements in the extension.

---

9. Prove that a finite commutative integral domain D is a field.

SOLUTION:

To say that D is a finite commutative integral domain means that D is a commutative ring with identity, has no zero divisors, and happens to have a finite number of elements. To establish that D is a field, we must show that any nonzero element has a multiplicative inverse. Let $x \in D$ be nonzero. Consider the set $\{ x^k : k \geq 1 \}$ consisting of products of x with itself. This subset of D does not contain 0 (else x would be a zero divisor). Since the set is finite, we have $x^k = x^l$ for some $k < l$. Thus $x^k = x^k x^{l-k}$ and so $x^k - x^k x^{l-k} = x^k(1 - x^{l-k}) = 0$; but $x^k \neq 0$ and we have no zero divisors, thus $1 - x^{l-k} = 0$ or simply $x^{l-k} = 1$. Thus, to each nonzero element $x \in D$ corresponds a power $k_x \geq 1$ such that $x^{k_x} = 1$; we now see that x has an inverse, namely the element $x^{k_x - 1}$.

---

10. Let H be a normal subgroup of a finite group G. Prove that H is a maximal (with respect to set inclusion) proper normal subgroup of G if and only if G/H is a nontrivial simple group.

SOLUTION:

Let H be a maximal proper normal subgroup. Then G/H is not trivial. By the correspondence theorem, subgroups of G/H are of the form K/H where $H \leq K \leq G$, and furthermore, K/H is normal in G/H if and only if K is normal in G. Let the subgroup K/H be normal; then K is normal in G and thus, by the maximality of H, either $K = H$ or $K = G$; thus the subgroup K/H is either the trivial subgroup or the entire quotient group, and thus the quotient group is simple.

Let G/H be a nontrivial simple group. Then H is a proper normal subgroup of G. I wish to show that H is maximal. Assume on the contrary that $H < K < G$ with $K \lhd G$; then the correspondence theorem says that $H/H < K/H < G/H$ and $K/H \lhd G/H$, contradicting the simplicity of G/H.

11. Give an example of a commutative integral domain that is not a principal ideal domain. Prove that your example works.

SOLUTION:

Consider $\mathbb{Z}[x]$. The ideal $(2, x)$ consists of all nonconstant polynomials and also the even constant polynomials. If this ideal were generated by a single element, to obtain the even constant polynomials but not the constant 1, the generator has to be 2 or -2; but then the ideal is missing the polynomial x. Thus it can't be principal.

12. Give an example of a prime ideal that is not a maximal ideal in a commutative ring.

SOLUTION:

In any commutative ring with identity, the zero ideal is a prime ideal precisely when the ring is nontrivial and has no nontrivial zero divisors; that is, the zero ideal is prime precisely when the ring is an integral domain. In an integral domain, the zero ideal is maximal precisely when the ring is a field. Thus, whenever one considers an integral domain that is not a field, for example the ring $\mathbb{Z}$ of integers, then the zero ideal is an example of a prime ideal that is not maximal. Less trivial examples are given below.

In $\mathbb{Z}[x]$, the ideal (x) is prime; after all, if a product of two polynomials gives a non-constant polynomial, then one of them had to be non-constant to begin with. However, the ideal (x) is not maximal because $(2, x)$ is larger and still proper.

In $\mathbb{Q}[x, y]$, the ideal (x) is prime and properly contained in the maximal ideal (x, y).

13. Let V be a vector space over a field F. Define "V is finite dimensional". Give an example of an infinite dimensional vector space over the field of real numbers.

14. Let V be the vector space over $\mathbb{R}$ consisting of polynomials $f(x) \in \mathbb{R}[x]$ of degree ≤ 6 with $f(1) = 0$. Exhibit a basis for V.

SOLUTION:

We know that $f(1) = 0$ precisely when $x-1$ is a factor of $f(x)$. Hence each polynomial in V is of the form $f(x) = (x-1)g(x)$, where $g(x) \in \mathbb{R}[x]$ is an arbitrary polynomial of degree ≤ 5. Here is my basis: $\{\, x-1, (x-1)x, (x-1)x^2, (x-1)x^3, (x-1)x^4, (x-1)x^5 \,\}$. ∎

15. Let $T: \mathbb{R}^2 \to \mathbb{R}^2$ be a linear transformation satisfying $T^2 = T$. Show that up to similarity there are exactly three such transformations. For each such T, find the dimension of the kernel and the dimension of the image.

SOLUTION:

I am given that T satisfies the polynomial $X^2 - X = X(X-1)$. Hence the minimal polynomial of T is either X, $X-1$, or $X(X-1)$. I shall consider each case separately:

- If the minimal polynomial is X, then T must be the zero transformation; its kernel has dimension 2 and its image has dimension 0.
- If the minimal polynomial is $X-1$, then T must be the identity transformation; its kernel has dimension 0 and its image has dimension 2.
- If the minimal polynomial is $X(X-1)$, then T has two distinct eigenvalues, namely 0 and 1; eigenvectors belonging to distinct eigenvalues are necessarily independent; thus, fixing an eigenvector for each, I obtain a basis of eigenvectors; in this basis, the matrix of T is diagonal with the eigenvalues on the diagonal. Put another way, up to similarity, T is the transformation given by that diagonal matrix in the original basis. At any rate, the kernel is precisely the eigenspace of 0; hence the kernel has dimension 1 and the image has dimension 1.

16. Give an example of a map $T: \mathbb{R}^3 \to \mathbb{R}^3$ that is *not* a linear transformation. Give an example of an invertible linear transformation $T: \mathbb{R}^2 \to \mathbb{R}^2$ that sends every one-dimensional subspace to a different one-dimensional subspace.

SOLUTION:

The map $(x,y,z) \mapsto (x,y,z+1)$ does not fix the origin, hence cannot be linear. The rotation map $(x,y) \mapsto (x\cos\theta - y\sin\theta, x\sin\theta + y\cos\theta)$ will send every one-dimensional subspace to a different one-dimensional subspace whenever the angle θ is nonzero. The inverse map is obtained by negating the angle.

By the way, here is how I remember the trigonometric expression for the rotation map. In terms of complex numbers, rotation by θ is simply multiplication by $e^{i\theta} = \cos\theta + i\sin\theta$. Each complex number $a+ib$ induces a multiplication map $\mathbb{C} \to \mathbb{C}$; if we replace $\mathbb{C}$ by $\mathbb{R}^2$ in the usual way, then the matrix of the multiplication-by-$(a+ib)$ map is the 2×2 matrix whose first column has the components of $a+ib$ and whose second column has the components of $i(a+ib)$:

$$\begin{bmatrix} a & -b \\ b & a \end{bmatrix}.$$

In particular, multiplication-by-$(e^{i\theta})$ is given by the matrix

$$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}.$$

Finally, the result of applying this matrix to the column vector (x,y) is the column vector $(x\cos\theta - y\sin\theta, x\cos\theta + y\sin\theta)$.

---

17. Determine all values of t so that -1 is an eigenvalue of the matrix

$$M = \begin{bmatrix} -5 & t \\ 12 & 5 \end{bmatrix}.$$

SOLUTION:

The characteristic polynomial of this matrix is $(\lambda+5)(\lambda-5) - 12t = \lambda^2 - 12t - 25$. This has a root of -1 precisely when $\lambda+1$ is a factor. Performing long division leaves the remainder $-12t-24$, which vanishes precisely when $t=-2$.

---

18. For which values of q are the vectors $(1,1,0)$, $(1,-1,0)$, and $(0,0,3)$ linearly independent over the finite field $\mathbb{F}_q$ of q elements?

SOLUTION:

The three column vectors are linearly independent precisely when the matrix composed by them has full rank; a square matrix has full rank precisely when its determinant is nonzero. The determinant is -6, which is nonzero when the characteristic of the field is ≥ 5. Since q must be a prime power to begin with, we must have $q = p^k$ with $p \geq 5$.

---

19. Let V be finite-dimensional over the field of complex numbers. Prove that a linear transformation $T\colon V \to V$ with 0 as the *only* eigenvalue is nilpotent (meaning $T^k = 0$ for some natural number k). Now suppose T is an arbitrary nilpotent transformation. Is $I - T$ invertible? Why or why not?

---

20. Let $T\colon V \to V$ be a linear transformation of the vector space V; let $\lambda_1, \ldots, \lambda_k$ be pairwise distinct eigenvalues of T; let v_i denote an eigenvector for λ_i, $1 \leq i \leq k$. Prove that $v_1, \ldots, v_k$ are linearly independent.

PROBLEMS FROM EXAM GIVEN AT LOUISIANA STATE UNIVERSITY ON 4 APRIL 1990

---

1. Let $\phi\colon G \to H$ be a homomorphism of groups.
(a) Show that $\mathrm{Ker}(\phi)$ is a normal subgroup of G.

(b) Show that $\text{IMAGE}(\phi)$ is a subgroup of H.

SOLUTION:

(a) The solution appears in the sample problems above.

(b) Since $\phi(1_G) = 1_H$, certainly $\text{IM}(\phi)$ is nonempty. Let $\phi(a), \phi(b)$ be in $\text{IM}(\phi)$. Then $\phi(a)\phi(b)^{-1} = \phi(ab^{-1})$, being the image of ab^{-1}, is in $\text{IM}(\phi)$.

---

2. Let R be a commutative ring with identity.

(a) Define "P is a prime ideal of R".

(b) Define "M is a maximal ideal of R".

(c) Show that P is a prime ideal of R if and only if R/P is an integral domain.

SOLUTION:

(a) A proper ideal P is **prime** if whenever $ab \in P$, then either $a \in P$ or $b \in P$. The texts I have most recently studied consider the zero ideal to be prime; this usage may not be universal.

(b) A proper ideal M is **maximal** if there is no ideal properly contained between M and R.

(c) Let P be a prime ideal. Since R is a commutative ring with identity, also R/P is a commutative ring with identity. Thus, to show that R/P is an integral domain, it remains to be shown that R/P has no zero divisors. The elements of R/P are (additive) cosets. Thus we consider the equation $(a+P)(b+P) = ab+P = 0+P = P$. We have $ab \in P$ and thus either $a \in P$ or $b \in P$. In other words, if a product equals zero, then one of the factors must be zero. Thus there are no zero divisors and therefore R/P is an integral domain. For the other direction, given that R/P is an integral domain and given a product $ab \in P$, we get the equation $0 = ab + P = (a+P)(b+P)$, and since there are no zero divisors, either $a \in P$ or $b \in P$. Thus P is a prime ideal.

---

3. Do the following.

(a) State the fundamental structure theorem for finitely generated modules over a principal ideal domain. (You may, if you wish, state it in the special case of abelian groups.)

(b) Find all non-isomorphic abelian groups of order 48.

SOLUTION:

(a) Let M be a finitely generated module over a principal ideal domain R. Let $n = \text{RANK}(M)$ be the minimal number of generators of M. (I use "free rank" for the rank of the free part of M, whereas many books use simply "rank"; their rank is thus not the same as my rank.) Then M has the structure

$$M \cong \frac{R}{I_1} \oplus \frac{R}{I_2} \oplus \cdots \oplus \frac{R}{I_n},$$

where $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subset R$. The first few ideals could well be the zero ideal, and certainly any ideal is principal and may be written in terms of a generator; this gives the formulation

$$M \cong R^d \oplus \bigoplus_{k=1}^{n-d} \frac{R}{(r_k)},$$

where $r_j \mid r_k$ for $j \leq k$, and R^d means $R \oplus \cdots \oplus R$. The portion "R^d" is the "free" part of the module and the exponent d is called the "free rank". The remaining portion is the "torsion" part. In the case that M is a finitely generated abelian group G, which should be thought of as a module over the principal ideal domain $\mathbb{Z}$, we have the structure

$$G \cong \mathbb{Z}^d \oplus \bigoplus_{k=1}^{n-d} \frac{\mathbb{Z}}{r_k\mathbb{Z}},$$

where the integers r_k divide each other in turns: $r_1 \mid r_2 \mid \cdots \mid r_{n-d}$.

(b) I seek a list of all non-isomorphic abelian groups of order $48 = 3 \cdot 2^4$. To shorten the notation, I shall use $\mathbb{Z}_{/n}$ to denote $\mathbb{Z}/n\mathbb{Z}$. The groups are $\mathbb{Z}_{/48}$, $\mathbb{Z}_{/24} \oplus \mathbb{Z}_{/2}$, $\mathbb{Z}_{/12} \oplus \mathbb{Z}_{/4}$, $\mathbb{Z}_{/12} \oplus \mathbb{Z}_{/2} \oplus \mathbb{Z}_{/2}$, $\mathbb{Z}_{/6} \oplus \mathbb{Z}_{/2} \oplus \mathbb{Z}_{/2} \oplus \mathbb{Z}_{/2}$.

---

4. Prove that $\mathbb{Z}[x]$ is *not* a Dedekind ring.

SOLUTION:

[WHAT IS A DEDEKIND RING?]

5. What is known to be the Fundamental Theorem of Galois Theory? Illustrate the theorem by an example.

SOLUTION:

Let E/F be a field extension of finite degree such that E is Galois over F. The Galois group $\text{Gal}(E/K)$ consists of automorphisms of E that fix K (pointwise). An intermediate field of E/F is a field K such that $F \subseteq K \subseteq E$. Given an intermediate field K, E/K is always Galois and the Galois group $\text{Gal}(E/K)$ is a subgroup of $\text{Gal}(E/F)$. The fundamental theorem of Galois theory states that there is a one-to-one inclusion-reversing correspondence between subgroups of the Galois group $\text{Gal}(E/F)$ and intermediate fields of E/F. That is, if one draws a lattice diagram (organized by inclusion) of the intermediate fields of E/F, and one draws an upside-down lattice diagram of the subgroups of $\text{Gal}(E/F)$, then these diagrams, as graphs, are identical; furthermore, vertices K in the former correspond to the subgroup $\text{Gal}(E/K)$ in the latter. The fundamental theorem says more. An intermediate field K is normal over the ground field F if and only if the corresponding subgroup $\text{Gal}(E/K)$ is normal in the full group $\text{Gal}(E/F)$; in that case, the intermediate field K is Galois over the ground, and its Galois group $\text{Gal}(K/F)$ is isomorphic to the quotient group obtained by taking $\text{Gal}(E/F)$ modulo $\text{Gal}(E/K)$.

For an example, consider the splitting field of x^3-2 over $\mathbb{Q}$. This is the degree 6 extension $\mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$, where $\sqrt[3]{2}$ denotes the real cube root of 2. The Galois group is S_3. Since the roots of x^3-2 form the vertices of a triangle in the complex plane, and since S_3 is also the dihedral group on 3 vertices, it is correct (and certainly convenient) to think of the Galois group as acting like the dihedral group. The rotation subgroup is cyclic of index 2 and thus is normal. The three reflections form subgroups of index 3, none of which is normal. There are precisely four (proper) intermediate fields of $\mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$ over $\mathbb{Q}$. They are $\mathbb{Q}(e^{2\pi i/3})$, $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(e^{2\pi i/3}\sqrt[3]{2})$, and $\mathbb{Q}(e^{4\pi i/3}\sqrt[3]{2})$. The Galois group of the top over $\mathbb{Q}(e^{2\pi i/3})$ is cyclic of order 3. The Galois group of the top over any of the other intermediate fields (the ones consisting of $\mathbb{Q}$ adjoined one of the three roots of x^3-2) is cyclic of order 2. Furthermore, $\mathbb{Q}(e^{2\pi i/3})$ is Galois over $\mathbb{Q}$ (it's the splitting field of x^2+x+1), and its Galois group over $\mathbb{Q}$ is cyclic of order 2; this is precisely the quotient group of S_3 by the normal subgroup generated by (123).

6. Let $K \subseteq \mathbb{C}$ be the smallest field that contains all roots of the polynomial $f(x) = x^3 - 2$. Clearly K is a vector space over $\mathbb{Q}$. Find $\text{Dim}_{\mathbb{Q}}(K)$.

SOLUTION:

The degree of the splitting field is 6. The roots of x^3-2 lie in a circle of radius $\sqrt[3]{2}$ in the complex plane. Adjoining the real root $\sqrt[3]{2}$ gives us a degree 3 extension that is a subfield of the real numbers; thus we are missing two roots and have the factorization $x^3-2 = (x-\sqrt[3]{2})(x^2+\sqrt[3]{2}x+\sqrt[3]{4})$. Adjoining another root gives us a degree 2 extension and we get the last root for free. Combining the two, we see that the splitting field has degree 6 over $\mathbb{Q}$; that is, $\text{Dim}_{\mathbb{Q}}(K) = 6$.

7. Consider the ring $\mathbb{Z}[i] = \{\, a+bi \mid a, b \in \mathbb{Z} \,\}$ of Gaussian integers. Answer the following and give justifications.

(a) Is $\mathbb{Z}[i]$ an integral domain?
(b) Is $\mathbb{Z}[i]$ a Unique Factorization Domain?
(c) Is $\mathbb{Z}[i]$ a Principal Ideal Domain?
(d) Is $\mathbb{Z}[i]$ a Euclidean Domain?

SOLUTION:

Because the answer to parts (a) and (d) is "yes", it follows, since every Euclidean domain is a principal ideal domain and every principal ideal domain is a unique factorization domain, the answer to parts (b) and (c) is also "yes". Thus it remains to be shown that $\mathbb{Z}[i]$ is an integral domain that happens to be Euclidean.

The former follows immediately from the fact that $\mathbb{Z}[i]$ is a subring of the field $\mathbb{C}$ of complex numbers. However, we can also use the definition. The addition and multiplication are defined by

$$(a+bi)+(c+di) = (a+c)+(b+d)i, (a+bi)(c+di) = (ac-bd)+(ad+bc)i.$$

One easily sees that the multiplication is commutative and that the element $1 = 1+0i$ is the multiplicative identity element. Let $(a+bi)(c+di) = 0$. Then $ac-bd = 0$ and $ad+bc = 0$. If $a \neq 0$, then $c = bd/a$ and thus $ad+bc = ad+b^2d/a = 0$; thus $d(a^2+b^2) = 0$ and, since $a^2+b^2 \geq a^2 > 0$, we must have $d = 0$, and thus also $c = 0$.

If $b \neq 0$, then $d = ac/b$ and $ad + bc = a^2c/b + bc = 0$; thus $c(a^2 + b^2) = 0$ and, as before, we conclude $c = 0$, and thus also $d = 0$. What we have shown is that if the first factor $a + bi$ of a zero product is nonzero, then the second factor must be zero. Thus there are no zero divisors.

To show that $\mathbb{Z}[i]$ is Euclidean, we need a "remainder function" defined on nonzero elements and taking values in the nonnegative integers. The Gaussian norm $d(a + bi) = a^2 + b^2 = (a + bi)(a - bi)$, being the square of the complex norm, will do just fine. Given two elements $a + bi$ and $c + di \neq 0$, we must show the existence of a quotient $p + qi$ and a remainder $r + si$ such that $a + bi = (p + qi)(c + di) + (r + si)$ with the additional condition that either $r + si = 0$ or else $d(r + si) < d(c + di)$. To solve this problem, we view $\mathbb{Z}[i]$ as a subring of the complex numbers, we view $\mathbb{Z}$ as an order-preserving subring of the real numbers, and we think of the Gaussian norm as the square of the complex norm. Then we are in a position to use elementary analytical techniques. This approach is followed here. Over the complexes we have the exact quotient $p' + q'i$ satisfying $a + bi = (p' + q'i)(c + di)$. There exists $p + qi$ such that $|p - p'| \leq \frac{1}{2}$ and $|q - q'| \leq \frac{1}{2}$; usually there is only one such choice, but there can be as many as four. Then $\big|(p + qi) - (p' + q'i)\big|^2 \leq \frac{1}{2}$. Now $r + si = (p' + q'i)(c + di) - (p + qi)(c + di) = (p'c - q'd - pc + qd) + (p'd + q'c - pd - qc)i = (p' - p)c + (q - q')d + (p' - p)di + (q' - q)ci = (p' - p)(c + di) + (q' - q)(c + di)i = (c + di)\big((p' - p) + (q' - q)i\big) = (c + di)\big((p' + q'i) - (p + qi)\big)$. We apply the Gaussian norm function to both sides by multiplying each side by its conjugate. This gives $d(r + si) =\leq \frac{1}{2}d(c + di)$ and thus we are done.

[I SHOULD ALSO BE ABLE TO DO THIS WITHOUT EMBEDDING IN THE COMPLEXES.]

Finally, although parts (b) and (c) follow from parts (a) and (d), I will at least discuss part (b) a little. Although $\mathbb{Z}[i]$ is a unique factorization domain, the set of primes is not the same as that in $\mathbb{Z}$. Here is what happens. The primes in $\mathbb{Z}$ which are congruent to 3 modulo 4 remain prime in $\mathbb{Z}[i]$. The primes in $\mathbb{Z}$ congruent to 1 modulo 4 split into a product of two primes in $\mathbb{Z}[i]$. The prime $2 \in \mathbb{Z}$ splits as a unit times the square of a prime in $\mathbb{Z}[i]$. This fully exhausts the primes in $\mathbb{Z}[i]$.

---

8. Let $T\colon V \to V$ be a linear transformation, where $\mathrm{DIM}_{\mathbb{C}}(V) = 5$ and T has minimum polynomial $(x - 1)^2(x + 1)$. Find all possible Jordan canonical forms for T.

---

9. Find the characteristic polynomial, minimum polynomial, and Jordan canonical form of the linear transformation T with matrix

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

---

10. Let $T\colon V \to V$ be a linear transformation. Show that T is diagonalizable if and only if V has a basis consisting of eigenvectors of T.

---

11. Let $T\colon V \to V$ be a linear transformation, and regard V as a $\mathbb{C}[x]$-module via T (that is, define $x(v) = T(v)$). Suppose that the minimum polynomial of T has degree equal to the dimension of V. Show that V is a cyclic $\mathbb{C}[x]$-module.

---

12. Let p be a prime number and let V be a 2-dimensional vectorspace over the field with p elements.
(a) Find the number of linear transformations $T\colon V \to V$.
(b) Find the number of invertible linear transformations $T\colon V \to V$.

PROBLEMS FROM EXAM GIVEN AT LOUISIANA STATE UNIVERSITY ON 19 NOVEMBER 1990

---

1. A finite group G of order p^n (p a prime, $n \geq 1$) operates on a finite set S whose order is relatively prime to p. Show that G has a fixed point on S.

SOLUTION:

Fixed points are merely orbits of size 1. The size of an orbit is the index of its stabilizer; the index of a subgroup divides the order of the group; thus, the size of an orbit divides p^n. The orbits partition the set S. If there is no fixed point, then every orbit has size some multiple of p, and thus their sum, namely the size of S, is also a multiple of p; but this is impossible since the size of S is relatively prime to p. Thus there must be a fixed point. (In fact, consider the remainder upon division of $|S|$ by p; the number of fixed points is some (possibly zero) multiple of p plus this remainder.)

---

2. Do the following.
(a) Find all the ideals in the ring $\mathbb{Z}/24\mathbb{Z}$.
(b) Find all the ideals in the ring $\mathbb{Q}[X]/(X^2 + X - 2)$.

SOLUTION:

(a) Note that $\mathbb{Z}/n\mathbb{Z}$ is always a principal ring (i.e., each ideal is principal), even when n isn't prime. The ideals of $\mathbb{Z}/24\mathbb{Z}$ are (0), (1), (2), (3), (4), (6), (8), and (12).

(b) Note that $X^2 + X - 2 = (X-2)(X+1)$. The ideals $(X-2)$ and $(X+1)$ are coprime, and thus the Chinese Remainder Theorem applies to give me $\mathbb{Q}[X]/(X^2+X-2) \cong \mathbb{Q}[X]/(X-2) \oplus \mathbb{Q}[X]/(X+1) \cong \mathbb{Q} \oplus \mathbb{Q}$. (The latter isomorphisms are evaluation maps.) The only ideals in $\mathbb{Q}\oplus\mathbb{Q}$ are (0), $(0)\oplus\mathbb{Q}$, $\mathbb{Q}\oplus(0)$, and $\mathbb{Q}\oplus\mathbb{Q}$. Backing up through the latter isomorphism, these ideals are $(0) = (X-2) \oplus (X+1)$, $(0) \oplus \mathbb{Q}[X]/(X+1) = (X-2) \oplus \mathbb{Q}[X]/(X+1)$, $\mathbb{Q}[X]/(X-2) \oplus (0) = \mathbb{Q}[X]/(X-2) \oplus (X+1)$, and $\mathbb{Q}[X]/(X-2) \oplus \mathbb{Q}[X]/(X+1)$. Finally, back in the original ring, these ideals are $(0) = (X^2+X-2)$, $(X-2)$, $(X+1)$, and $\mathbb{Q}[X]/(X^2+X-2)$.

---

3. Let $\mathbb{F}_3$ be the finite field with 3 elements.
(a) Explain why the polynomial $X^3 + 2X + 1$ is irreducible over $\mathbb{F}_3$.
(b) The finite field $\mathbb{F}_3[X]/(X^3+2X+1)$ has 27 elements. Call this field $\mathbb{F}_{27}$. Write the multiplicative inverse of $-2 + \overline{X}$ in the form $a + b\overline{X} + c\overline{X}^2$, where $a, b, c \in \mathbb{F}_3$ and $\overline{X}$ denotes the residue class of X.
(c) The Galois group $\mathrm{GAL}(\mathbb{F}_{27}/\mathbb{F}_3)$ is known to be cyclic of order 3, generated by a canonical element $\sigma\colon \mathbb{F}_{27} \to \mathbb{F}_{27}$ called the Frobenius. Write $\sigma(\overline{X})$ and $\sigma(\overline{X}^2)$ each in the form $a + b\overline{X} + c\overline{X}^2$, where $a, b, c \in \mathbb{F}_3$.

SOLUTION:

(a) If the polynomial $p(X) = X^3 + 2X + 1$ factors, then it splits off a linear factor. Since linear factors correspond to roots, we can check whether it splits off a linear factor by checking whether it has any roots; over $\mathbb{F}_3$, there are three numbers to check; but $p(0) = 1$, $p(1) = 1$, and $p(2) = 1$; thus there are no roots and thus the polynomial is irreducible.

(b) To find the inverse of $-2 + \overline{X} = 1 + \overline{X}$, we use long division. Write the element 1 as $X^3 - X - 1$. Dividing this by $X + 1$ gives the quotient $X - X^2$. Thus the inverse is $0 + \overline{X} - \overline{X}^2$.

(c) The Frobenius is $\sigma\colon x \mapsto x^3$. Thus $\sigma(\overline{X}) = X^3 = -1 - 2X$, and $\sigma(\overline{X}^2) = X^6 = 1 + \overline{X} + \overline{X}^2$.

---

4. Do the following.
(a) Show that the ring $\mathbb{Z}[X]$ is not a principal ideal domain.
(b) Describe all the prime ideals in $\mathbb{Z}[X]$.

SOLUTION:

(a) The ideal $(2, X)$ in $\mathbb{Z}[X]$ is not principal.

(b) The prime ideals in $\mathbb{Z}[X]$ are (0), (p), $(f(X))$, and $(p, f(X))$, where p is a prime and $f(X)$ is an irreducible polynomial.

[IS THIS CORRECT? HOW DO I KNOW THERE AREN'T ANY MORE?]

5. Let k be a field. Consider the ring homomorphism $\phi: k[x,y] \to k[t]$ given by $\phi(x) = t^2$ and $\phi(y) = t^3$.

(a) Write down one element $f(x,y) \in k[x,y]$ in the kernel of ϕ.

(b) Show that there is a ring homomorphism $\bar{\phi}: k[x,y]/\mathrm{Ker}(\phi) \to k[t]$ induced by ϕ. Is $\bar{\phi}$ injective? Is it surjective? Prove your assertions.

(c) Give generators for the ideal $\mathrm{Ker}(\phi)$.

SOLUTION:

(a) Other than 0, an element in the kernel of ϕ is $x^3 - y^2$.

(b) The ring homomorphism $\bar{\phi}: k[x,y]/\mathrm{Ker}(\phi) \to k[t]$ is defined by $\bar{\phi}(f(x,y) + \mathrm{Ker}(\phi) = \phi(f(x,y)) = f(t^2, t^3)$. This map is well-defined since, given two different representatives of a coset, their difference lies in $\mathrm{Ker}(\phi)$ and thus maps to 0, and thus the images of the two representatives are equal. The homomorphism properties follow from the properties of ϕ. The induced map $\bar{\phi}$ is injective since the difference of two equal images is zero and thus the difference of the preimages lies in $\mathrm{Ker}(\phi)$ and thus the preimages are equal in $k[x,y]/\mathrm{Ker}(\phi)$. However, the induced map $\bar{\phi}$ is not surjective, as can be seen by noting that $t \in k[t]$ is not in the image.

(c) The ideal $\mathrm{Ker}(\phi)$ is generated by polynomials of the form $x^{3j} - y^{2j}$, where $j \geq 1$ is odd.

[IS THIS CORRECT?]

---

6. Do the following.

(a) Write down all the abelian groups (up to isomorphism) of order 2700.

(b) Give one example of a non-abelian group of order 12. Verify that your example is indeed non-abelian.

SOLUTION:

(a) Since $2700 = 2^2 3^3 5^2$, the list of non-isomorphic abelian groups of order 2700 is $\mathbb{Z}/2700\mathbb{Z}$, $\mathbb{Z}/1350\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/540\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/900\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/300\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}$, $\mathbb{Z}/300\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/270\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$, $\mathbb{Z}/450\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/180\mathbb{Z} \oplus \mathbb{Z}/15\mathbb{Z}$, $\mathbb{Z}/90\mathbb{Z} \oplus \mathbb{Z}/30\mathbb{Z}$, $\mathbb{Z}/150\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z}$, $\mathbb{Z}/60\mathbb{Z} \oplus \mathbb{Z}/45\mathbb{Z}$. (Maybe I screwed up the list, but at any rate there should be twelve of them.)

(b) The dihedral group on 6 vertices has order 12 and is not abelian. This is the group $\langle a, b : a^6 = b^2 = abab = 1 \rangle$. For example, $ab \neq ba$ since in fact $ab = ba^{-1}$.

---

7. Let α and β be conjugate elements of the symmetric group S_n. Suppose α fixes at least two symbols. Prove that α and β are conjugate via an element γ of the alternating group A_n.

SOLUTION:

We have $\alpha = \gamma\beta\gamma^{-1}$. Since we can relabel the symbols in S_n, we may assume that α fixes $\{1, 2\}$. Thus α lies in $\mathrm{Stab}(1)$ and $\mathrm{Stab}(2)$.

[LEARN MORE ABOUT ACTIONS.]

---

8. Are $(13)(25)$ and $(12)(45)$ conjugate in S_5? If you say "yes", then find an element giving the conjugation. If you say "no", then prove your answer.

SOLUTION:

In general, two elements are conjugate if and only if they have the same cycle type. Thus the answer is "yes". The conjugation is given by (243), since $(243)(13)(25)(234) = (12)(45)$.

---

9. Let $T: V \to W$ be a linear transformation between k-vectorspaces, where k is any field. Let $\{v_1, \ldots, v_s\}$ be a set of vectors of V and $r \leq s$ an index such that $\{v_1, \ldots, v_r\}$ is a basis of $\mathrm{Ker}(T)$, and $\{T(v_{r+1}), \ldots, T(v_s)\}$ is a basis of $\mathrm{Im}(T)$. Show that $\{v_1, \ldots, v_s\}$ is a basis of V.

---

10. Let k be an algebraically closed field of characteristic zero. Write down all the equivalent Jordan canonical forms of 5×5 matrices with coefficients in k whose minimal polynomial is

$$m(\lambda) = (\lambda - 1)^2(\lambda + 2)^2.$$

11. Let $T: \mathbb{Q}^3 \to \mathbb{Q}^3$ be the linear transformation expressed relative to the standard basis $e_1 = (1, 0, 0)$, $e_2 = (0, 1, 0)$, $e_3 = (0, 0, 1)$ by the matrix

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

(a) Find a basis for $\mathrm{KER}(T)$.
(b) Find a basis for $\mathrm{IM}(T)$.
(c) Find the matrix expressing T relative to the basis $f_1 = (-1, 1, 0)$, $f_2 = (0, 1, -1)$, $f_3 = (1, 0, 1)$.

PROBLEMS FROM EXAM GIVEN AT LOUISIANA STATE UNIVERSITY ON 10 APRIL 1991

1. Let G be a group.
(a) Define the commutator subgroup G' of G.
(b) Show that if $\phi: G \to H$ is a group homomorphism and H is an abelian group, then $G' \leq \mathrm{KER}(\phi)$.

SOLUTION:

(a) The commutator subgroup is the subgroup generated by all commutators; that is, it is the smallest subgroup containing all elements of the form $aba^{-1}b^{-1}$. Note that this subgroup, which is always normal, generally consists of more than just commutators. It has the additional property of being the smallest normal subgroup such that the quotient group G/G' is abelian.

(b) Consider the image of a commutator under the mapping ϕ. We have $\phi(aba^{-1}b^{-1}) = \phi(a)\phi(b)\phi(a)^{-1}\phi(b)^{-1}$, and this is just e since H is abelian. Thus all commutators lie in $\mathrm{KER}(\phi)$, and thus the smallest subgroup generated by the commutators, namely G', also lies in $\mathrm{KER}(\phi)$.

2. Show that there are no simple groups of order 104.

SOLUTION:

Let G be a group of order $104 = 2^3 \cdot 13$. The number of 13-Sylow subgroups, which is congruent to 1 modulo 13 and also divides 8, must be 1. Thus this subgroup is normal and thus G is not simple.

3. Let p be a prime number.
(a) List, up to isomorphism, all abelian groups of order p^3.
(b) Let F be a field with p^3 elements. The additive group of F is an abelian group of order p^3. Identify this group from your list in part (a) and justify your answer.

SOLUTION:

(a) Every group of order p is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. A complete list of non-isomorphic abelian groups of order p^3 is $\mathbb{Z}/p^3\mathbb{Z}$, $\mathbb{Z}/p^2\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$, and $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$.

(b) There exists (up to isomorphism) precisely one field with p^3 elements. This field can be constructed by taking $\mathbb{Z}/p\mathbb{Z}[x]$ modulo the ideal generated by any degree 3 irreducible polynomial. The resulting structure is a vector space of dimension 3 over $\mathbb{Z}/p\mathbb{Z}$. That is, the elements of the field are in one-to-one correspondence with triplets of numbers in $\mathbb{Z}/p\mathbb{Z}$ and the addition is performed coordinate-wise. (The multiplication, however, is not performed coordinate-wise.) Thus we see that the additive group of the field is $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$.

---

4. Do the following.

(a) Let G be a group. Define the center $Z(G)$ of G.

(b) Show that every element of the symmetric group S_5 is conjugate to exactly one of the permutations (12), (123), (1234), (12345), $(12)(345)$, $(12)(34)$, or the identity e.

(c) Show that $Z(S_5) = \{e\}$.

SOLUTION:

(a) The center of G is the normal subgroup $Z(G) = \{\, z \in G \mid zg = gz \text{ for all } g \in G \,\}$. In words, the center is the set of those elements that commute with the entire group; this set happens to be a normal subgroup.

(b) What must be established is that two elements are conjugate if and only if their cycle types are identical. Since each cycle type is represented precisely once in the list in part (b), the result will be established. The crux of the argument is that conjugating an element α (written as disjoint cycles) by β has the effect of applying the permutation β individually to each entry of each cycle of α; thus, cycle type is preserved, and furthermore, given two elements of equal cycle type, we see how to construct the conjugation. The best way to see that the crux holds is not to get bogged down in symbols but instead to note that conjugation has the effect of a temporary relabeling. Rather than applying α, you first relabel the set $\{\, 1, \ldots, n \,\}$ using β^{-1}, then you apply α to the relabeled set, and then you restore the labeling using β. The net effect is that the permutation has the original structure, only some of the symbols have been relabeled.

(c) Another way to think of the center is all elements z which fix the entire group pointwise under conjugation. As we just saw, conjugation corresponds to a relabeling; any non-trivial relabeling moves at least two symbols, say 1 and 2. If it swaps them, then this relabeling does not fix (13) under conjugation. Else, it does not fix (12) under conjugation. Thus, as long as there are three or more symbols, then the only relabeling which fixes all elements under conjugation is the trivial relabeling. In particular, with five symbols, this is the case. Thus $Z(S_5) = \{e\}$.

---

5. Let R be a commutative ring with identity and let I and J be ideals of R.

(a) Define what is meant by the sum $I + J$ and product IJ of the ideals I and J.

(b) If I and J are distinct maximal ideals, show that $I + J = R$ and $I \cap J = IJ$.

SOLUTION:

(a) The sum $I+J$ is the ideal generated by elements of the form $i+j$ where $i \in I, j \in J$; the product IJ is the ideal generated by elements of the form ij where $i \in I, j \in J$. It so happens that the sum $I+J$ is just $\{\, i+j \mid i \in I,\ j \in J \,\}$, for this is already an ideal. With the product, however, it's a bit more complicated. The set $\{\, ij \mid i \in I,\ j \in J \,\}$ is generally not already an ideal; the ideal generated by this set consists of all finite sums of these elements; thus $IJ = \{\, \sum_{k=1}^{n} i_k j_k \mid i_k \in I,\ j_k \in J,\ n \geq 1 \,\}$. Since $I + J$ contains I and J, and any ideal containing I and J also contains $I + J$, we see that $I + J$ is the smallest ideal containing both I and J. Since the generators of IJ are contained in both I and J, we see that $IJ \subseteq I \cap J$.

(b) By definition, a maximal ideal is a proper ideal such that no ideal sits between it and the entire ring. If I and J are distinct maximal ideals, then there are elements in I that are not in J; thus $I + J$, the smallest ideal containing both I and J, properly contains I and thus must be the entire ring. Since we always have $IJ \subseteq I \cap J$, we must show $I \cap J \subseteq IJ$. Let $x \in I \cap J$. [HMM]

[FINISH THIS.]

---

6. Let R be an integral domain.

(a) For $a \in R$, define what is meant for a to be an "irreducible" element and for a to be a "prime" element.

(b) Show that if a is a prime element, then a is an irreducible element.

(c) Let $R = \mathbb{Z}[\sqrt{-5}] = \{\, m + \sqrt{-5}n \mid m, n \in \mathbb{Z} \,\}$. Show that 2 is an irreducible element of R that is not prime. (Hint: The function $N\colon R \to \mathbb{Z}$ given by $N(m + \sqrt{-5}n) = m^2 + 5n^2$ may be useful.)

SOLUTION:

(a) A element $a \in R$ is **irreducible** if whenever $a = bc$, one of b, c is a unit. A element $a \in R$ is **prime** if $a \neq 0$ and if whenever $a \mid bc$, either $a \mid b$ or $a \mid c$.

(b) Let a be prime and let $a = bc$. Then $a \mid bc$ and thus either $a \mid b$ or $a \mid c$; without loss of generality, let's assume the former. Then $b = ad$, and thus $a = adc$. Then $a(1-dc) = 0$ and since $a \neq 0$, we have $dc = 1$. Thus c is a unit, and thus a is irreducible.

(c) Call the function N the "norm"; it may be defined as $N(m+\sqrt{-5}n) = (m+\sqrt{-5}n)(m-\sqrt{-5}n)$. The norm preserves products since $N((m+\sqrt{-5}n)(r+\sqrt{-5}s)) = N(mr-5ns+\sqrt{-5}(nr+ms)) = m^2r^2 - 10mrns + 25n^2s^2 + 5n^2r^2 + 10nrms + 5m^2s^2 = m^2r^2 + 25n^2s^2 + 5n^2r^2 + 5m^2s^2 = (m^2+5n^2)(r^2+5s^2) = N(m+\sqrt{-5}n)\cdot N(r+\sqrt{-5}s)$. Furthermore, we have $N(1) = 1$. Thus we see that the norm of a unit is 1 since, if $bc = 1$, then $N(bc) = N(1) = 1 = N(b)\cdot N(c)$ and out of $N(b) = \pm 1$ only the positive value is a possibility. On the other hand, if $N(m+\sqrt{-5}n) = 1$, then $n = 0$ and $m = \pm 1$, and each possibility does give rise to a unit; thus, the only units in R are ± 1, and an element is a unit if and only if its norm is 1. Now we know enough about this function to make use of it. If 2 is reducible, then $2 = bc$ with neither of b, c being a unit. Thus $N(2) = N(b)\cdot N(c) = 4$; since neither $N(b)$ nor $N(c)$ can be 1, we have $N(b) = N(c) = 2$. But a quick glance at the norm function tells us that no ring element has norm 2. Thus our situation is impossible and the ring element 2 must be irreducible. However, it is not prime, since it divides $6 = (1+\sqrt{-5})(1-\sqrt{-5})$ but does not divide either factor.

---

7. Let R be a commutative ring with identity and let M be a nonzero R-module. If $x \in M$, the annihilator of x is the ideal of R defined by $\mathrm{Ann}_R(x) = \{\, a \in R \mid ax = 0 \,\}$.
(a) Show that $Rx \cong R/\mathrm{Ann}_R(x)$, where Rx is the submodule of M generated by x.
(b) If R is a principal ideal domain, show that there is an $x \in M$ for which $\mathrm{Ann}_R(x)$ is a prime ideal.

SOLUTION:

(a) Fix $x \in M$. Consider the map $\phi\colon R \to M$ defined by $\phi(r) = rx$. The image of this map is Rx. The kernel of this map is $\mathrm{Ann}_R(x)$. Thus $Rx \cong R/\mathrm{Ann}_R(x)$. **[Yes, but I need to show that this is the appropriate type of homomorphism. What properties must a module homomorphism possess?]**

(b) **[Hmm]**

---

8. Do the following.
(a) Let F be a field and let $f(X) \in F[X]$ be a polynomial of degree 3. Show that $f(X)$ is reducible in $F[X]$ if and only if $f(X)$ has a root in F.
(b) Give an example of a reducible polynomial $f(X) \in \mathbb{Q}[X]$ of degree 4 such that $f(X)$ has no root in $\mathbb{Q}$.

SOLUTION:

(a) If a degree 3 polynomial factors, then it splits off a linear factor. Linear factors correspond to roots. Thus, a degree 3 polynomial factors if and only if it has a root.

(b) The polynomial $x^4 + 2x^2 + 1 = (x^2+1)(x^2+1)$ factors over $\mathbb{Q}$ but does not have a root in $\mathbb{Q}$; the roots are $\pm i$ (each with multiplicity 2), and these do not lie in $\mathbb{Q}$.

---

9. If $A \in M_n(\mathbb{C})$ is a diagonalizable $n \times n$ complex matrix, show that A has a square root; that is, show that there is a matrix $B \in M_n(\mathbb{C})$ such that $B^2 = A$.

---

10. Let V be the complex vector space of polynomials $p(X) \in \mathbb{C}[X]$ of degree ≤ 4. Define a linear transformation $T\colon V \to V$ by $T(p(X)) = p''(X)$, where $p''(X)$ is the second derivative of the polynomial $p(X)$. Compute the characteristic polynomial, minimal polynomial, and Jordan canonical form of the linear transformation T.

---

11. Let V and W be finite dimensional vector spaces over a field F, and let $\mathrm{Hom}_F(V,W)$ denote the vector space of linear transformations from V to W. Let $\mathcal{B} = \{\, v_1, \ldots, v_n \,\}$ be a basis of V and let $\mathcal{C} = \{\, w_1, \ldots, w_m \,\}$ be a basis of W.
(a) Write down a basis of $\mathrm{Hom}_F(V,W)$ and verify that it is a basis.
(b) What is $\mathrm{Dim}_F(\mathrm{Hom}_F(V,W))$?

12. Let p be a prime number and let V be a vector space of dimension 3 over the field $\mathbb{Z}/p\mathbb{Z}$ with p elements. Suppose that $T: V \to V$ is a linear transformation such that the matrix of T relative to some basis of V is the matrix

$$A = \begin{pmatrix} 4 & 2 & 12 \\ 1 & -1 & 12 \\ 4 & 2 & -1 \end{pmatrix} \in M_3(\mathbb{Z}/p\mathbb{Z}).$$

Find all primes p for which T is *not* a linear isomorphism.

PROBLEMS FROM EXAM GIVEN AT LOUISIANA STATE UNIVERSITY ON 4 NOVEMBER 1991

1. Suppose $\phi: R \to S$ is a ring homomorphism.
(a) Show that $\mathrm{KER}(\phi)$, the kernel of ϕ, is an ideal of R.
(b) Show that ϕ is injective if and only if $\mathrm{KER}(\phi) = 0$.
(c) If ϕ is surjective, show that $R/\mathrm{KER}(\phi) \cong S$.

2. Do the following.
(a) Prove that the number of elements in a finite field must be p^n for some prime p.
(b) Show that $X^3 + X - 1$ is irreducible over $\mathbb{F}_5$.
(c) Construct a field with 125 elements.

3. Do the following.
(a) Suppose G is a group and $a, b \in G$ are elements whose orders are $|a| = m$ and $|b| = n$. Show that if $ab = ba$ and if m, n are relatively prime, then the order of ab is mn.
(b) Prove that an abelian group of order pq, where p and q are distinct primes, must be cyclic.
(c) Must a group of order mn be cyclic, where m and n are relatively prime? Justify your answer.

4. Do the following.
(a) Express $X^4 - 2X^2 - 3$ as a product of irreducible polynomials over each of the following fields: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/5\mathbb{Z}$.
(b) Give an example of a UFD that is not a PID and justify your answer.

5. Do the following.
(a) State the fundamental structure theorem for finitely generated modules over a PID. (If you can't state it in this generality, then do so in the special case of abelian groups.)
(b) Give a list of all (up to isomorphism) abelian groups of order 24.
(c) Give an example of a nonabelian group of order 24.

6. Let $\phi: G \to H$ be a surjective group homomorphism, and let N be a normal subgroup of G. Show that $\phi(N)$ is a normal subgroup of H. What happens if ϕ is not surjective? Explain your answer.

---

7. Let $G = SL_2(\mathbb{F}_3)$.

(a) Show that G has 24 elements.

(b) Let P be the subgroup of G generated by

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \qquad \text{and} \qquad B = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}.$$

Show that P is a 2-Sylow subgroup of G.

(c) Show that P is isomorphic to the quaternion group Q_8. Recall that Q_8 is the subgroup of $GL_2(\mathbb{C})$ generated by the matrices

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

---

8. Let R be an integral domain. Show that the group of units of the polynomial ring $R[X]$ is equal to the group of units of the ground ring R.

---

9. Let $\omega = (1 + \sqrt{-3})/2$ and let $R = \{\, a + b\omega \mid a, b \in \mathbb{Z} \,\}$.

(a) Show that R is a subring of $\mathbb{C}$.

(b) Show that R is a Euclidean ring with respect to the norm function $N(z) = z\bar{z}$ (here $\bar{z}$ means the complex conjugate of z).

---

10. Suppose V is a finite-dimensional vector space over a field k. Prove that the dual space of V is isomorphic to V.

---

11. Let A, B be square matrices with entries in a field K.

(a) Show that AB and BA have the same characteristic values.

(b) If A and B are similar, show that A and B have the same characteristic polynomial.

---

12. Do the following.

(a) Let A be the matrix

$$\begin{pmatrix} -4 & -2 & -4 \\ 4 & 2 & 4 \\ 2 & 1 & 2 \end{pmatrix}$$

over $\mathbb{Q}$. Show that A is nilpotent and determine the minimal polynomial of A, the characteristic polynomial of A, and the Jordan canonical form of A.

(b) Suppose a 6×6 matrix B over $\mathbb{C}$ has characteristic polynomial $(X-2)^4(X-3)^2$ and minimal polynomial $(X-2)^2(X-3)$. What are the possible Jordan canonical forms for B?

PROBLEMS FROM EXAM GIVEN AT LOUISIANA STATE UNIVERSITY ON 16 MARCH 1992

1. Let G be a (finite) p-group (i.e., $|G| = p^m$). Let G act as a group of transformations on a set X. Prove the following.
(a) For $x \in X$, the order of the orbit of x, $\left|\{\, gx \mid g \in G \,\}\right|$, is a power of p.
(b) If $p \nmid |X|$, then G has a fixed point in X (i.e., there exists $x \in X$ such that $gx = x$ for all $g \in G$).

2. Show that there are no simple groups of order 200.

3. Given the permutations $x = (12)(34)$ and $y = (56)(13)$, do the following.
(a) Find a permutation a such that $a^{-1}xa = y$.
(b) Prove that there does not exist a permutation a such that $a^{-1}(123)a = (13)(578)$.

4. Prove that the homomorphic image of a solvable group is solvable.

5. Show that $\mathbb{R}[x]/I$, where $\mathbb{R}$ is the field of real numbers and I is the ideal generated by an irreducible polynomial of degree 2, is isomorphic to the field $\mathbb{C}$ of complex numbers.

6. Show that in the ring M of 2×2 real matrices (with the usual addition and multiplication), the only 2-sided ideals are (0) and the entire ring.

7. Let R be a commutative ring with identity. Suppose $a \in R$ is a unit (i.e., it has a multiplicative inverse) and $b \in R$ is nilpotent (i.e., $b^r = 0$ for some sufficiently large integer r). Show that $a + b$ is a unit.

8. Do the following.
(a) Define "prime ideal" and "maximal ideal" in a commutative ring with identity R.
(b) Lef $F \colon R \to S$ be a ring homomorphism, where R and S are commutative rings with identity, and let P be a prime ideal of S. Show that $F^{-1}(P)$ is a prime ideal of R.
(c) Let F be as in part (b). If M is a maximal ideal of S, is $F^{-1}(M)$ a maximal ideal of R? If your answer is "yes", then prove it; if your answer is "no", then give a counterexample.

9. Let V and Z be vector spaces over a field F. Suppose $T \colon T \to Z$ is linear and onto, and let W be its null space. Prove that Z is isomorphic to V/W.

10. Let p be a prime; let $F_p = \mathbb{Z}/p\mathbb{Z}$ be the field with p elements; let $V = (F_p)^4$ be the 4-dimensional vector space over F_p; and, let W be the subspace of V spanned by the three vectors

$$\begin{aligned} a_1 &= (1, 2, 2, 1) \\ a_2 &= (0, 2, 0, 1) \\ a_3 &= (-2, 0, -4, 3). \end{aligned}$$

Find $\textsc{Dim}(W)$. (Hint: It depends on p.)

11. Do the following.
(a) Let A be an $n \times n$ matrix with complex coefficients. State a necessary and sufficient condition in terms of the minimal polynomial of A in order that A be diagonalizable.
(b) Show that an $n \times n$ matrix A with complex coefficients which satisfies $A^2 = A$ is diagonalizable.

12. Do the following.
(a) Let A be a complex 5×5 matrix with characteristic polynomial $f(x) = (x-2)^3(x+7)^2$ and minimal polynomial $p(x) = (x-2)^2(x+7)$. Find the Jordan normal form of A.
(b) Find all the invariant factors of A.

PROBLEMS FROM EXAM GIVEN AT LOUISIANA STATE UNIVERSITY ON 22 OCTOBER 1992

1. Do the following.
(a) Construct an isomorphism of rings

$$\phi\colon \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}/20\mathbb{Z}.$$

For your notation, let $[a]_n$ be the coset $a + n\mathbb{Z}$ in $\mathbb{Z}/n\mathbb{Z}$.
(b) Let $(\mathbb{Z}/20\mathbb{Z})^*$ be the multiplicative group of units in the ring $\mathbb{Z}/20\mathbb{Z}$. That is,

$$\left[x \in (\mathbb{Z}/20\mathbb{Z})^*\right] \iff \left[\exists y \in \mathbb{Z}/20\mathbb{Z} \text{ such that } xy = [1]_{20}\right].$$

Construct an isomorphism of abelian groups

$$\psi\colon \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \to (\mathbb{Z}/20\mathbb{Z})^*.$$

2. State the fundamental structure theorem for finitely generated modules over a principal ideal domain. Apply the theorem to find the number of (non-isomorphic) abelian groups of order 1000.

3. Let $\mathbb{F}_{11} = \mathbb{Z}/11\mathbb{Z}$ be the finite field with 11 elements.
(a) Show that the polynomial $x^2 + 1$ is irreducible over $\mathbb{F}_{11}$.
(b) Let α be a root of $x^2 + 1 = 0$ in an algebraic closure $\overline{\mathbb{F}}_{11}$ of $\mathbb{F}_{11}$. In the field $\mathbb{F}_{121} = \mathbb{F}_{11}(\alpha)$, express

$$\frac{1}{2 + 3\alpha}$$

in the form $a + b\alpha$, where $a, b \in \mathbb{F}_{11}$.
(c) Describe the Galois group of the extension $\mathbb{F}_{121}/\mathbb{F}_{11}$.

4. Do the following.
(a) Give an example of an integral domain that is not a unique factorization domain.
(b) Give an example of a unique factorization domain that is not a principal ideal domain.

---

5. Determine all the subgroups of S_3, the symmetric group on 3 symbols. Which os these is a normal subgroup?

---

6. Let p be an odd prime number. Describe (up to isomorphism) all groups of order $2p$.

---

7. The group H of quaternions consists of the symbols

$$1, -1, i, -i, j, -j, k, -k$$

with the relations $(-1)^2 = 1$, $i^2 = j^2 = k^2 = ijk = -1$, $i(-1) = (-1)i = -i$, $j(-1) = (-1)j = -j$, $k(-1) = (-1)k = -k$. Let $N = \{1, -1, i, -i\}$. Show that N is a normal subgroup of H. Describe the quotient group H/N.

---

8. Let K be a Galois extension of $\mathbb{Q}$ with Galois group $\mathrm{Gal}(K/\mathbb{Q}) = C_{22}$, the cyclic group of order 22.
(a) Find the degrees over $\mathbb{Q}$ of all subfields $F \subseteq K$.
(b) Give an explicit example of a field K with $\mathrm{Gal}(K/\mathbb{Q}) = C_{22}$.

---

9. Let $f\colon \mathbb{Z}^2 \to \mathbb{Z}/3\mathbb{Z}$ be the homomorphism $f(x, y) = x + y \pmod{3}$.
(a) Find a $\mathbb{Z}$-module basis for $K = \mathrm{Ker}(f)$.
(b) Does there exist a $\mathbb{Z}$-module homomorphism $g\colon \mathbb{Z}^2 \to K$ such that the composition $K \to \mathbb{Z}^2 \to K$ of g with the inclusion map is the identity? Why or why not?

---

10. Let $\alpha = \sqrt{2} + \sqrt{3}$. Show that the field $K = \mathbb{Q}(\alpha)$ has degree 4 over $\mathbb{Q}$. Determine the Galois group $\mathrm{Gal}(K/\mathbb{Q})$. Find the minimal polynomial of α over $\mathbb{Q}$.

---

11. Let V be a 2-dimensional vector space over the field $\mathbb{C}$ of complex numbers. Let $T\colon V \to V$ be the $\mathbb{C}$-linear endomorphism given, relative to some basis of V, by the matrix

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

(a) Write down the characteristic polynomial of T.
(b) Decompose V into a direct sum $\mathbb{C}v_1 \oplus \mathbb{C}v_2$, where v_1, v_2 are eigenvectors of T.

---

12. Let p be a prime number; let V be a 2-dimensional vector space over the finite field $\mathbb{F}_p$ of p elements. Find the number of linear transformations $T\colon V \to V$ with trivial kernel.

PROBLEMS FROM EXAM GIVEN AT LOUISIANA STATE UNIVERSITY ON 19 MARCH 1993

---

1. Show that the center of a p-group is non-trivial.

2. Let Q be the quaternion group of order 8.
(a) Show that there is an exact sequence:

$$\{1\} \to \mathbb{Z}_4 \to Q \to \mathbb{Z}_2 \to \{1\}.$$

(b) Show that no sequence as in (a) can split.

3. Let G be a group and H, K subgroups of G.
(a) Show that $[G : K] \geq [H : H \cap K]$.
(b) Show that if H, K are subgroups of finite index in G, then $H \cap K$ is a subgroup of finite index of G. (Hint: Use part (a).)

4. Let R be a commutative ring.
(a) Define "prime ideal" and "maximal ideal", and give an example of a prime ideal which is not maximal.
(b) Show that every maximal ideal is prime.
(c) Show that R/I is a field if and only if I is maximal.

5. Let R be a principal ideal domain and M an R-module. Let x, y be torsion elements of M with $\textsc{Ann}(x) = (p)$ and $\textsc{Ann}(y) = (q)$. Suppose that p, q are relatively prime. Show that $\textsc{Ann}(x + y) = (pq)$.

6. Find polynomials $p(x)$ and $q(x)$ so that

$$p(x) \cdot (x^3 - x^2 + x + 1) + q(x) \cdot (x^2 - 2x + 2) = 1.$$

7. Explicitly construct a field with 9 elements, and find a generator of the multiplicative group of this field.

8. Let $F = \mathbb{Q}(\omega, b)$, where $\mathbb{Q}$ denotes the rational numbers, $\omega^3 = 1$, $\omega \neq 1$, and b is the real cube root of 2.
(a) Show F has degree 6 over $\mathbb{Q}$.
(b) Show F contains a subfield F_1 with $[F_1 : \mathbb{Q}] = 3$ and the extension $F_1/\mathbb{Q}$ is *not* normal.
(c) Find the Galois group of F over $\mathbb{Q}$. (Hint: Use part (b).)

9. Show that every extension of $\mathbb{Q}$ of degree 2 is of the form $\mathbb{Q}(\sqrt{d})$ for some square-free integer $d \neq 0, 1$.

10. Consider an exact sequence of finite-dimensional vector spaces

$$\{0\} \to V_1 \to V_2 \to \cdots \to V_n \to \{0\}.$$

Show that

$$\sum_{i=1}^{n} (-1)^i \textsc{Dim}(V_i) = 0.$$

11. Let V be a vector space over the complex numbers $\mathbb{C}$. Let $T: V \to V$ be a linear transformation, and regard V as a $\mathbb{C}[x]$-module via T; i.e., define $x(v) := T(v)$.
(a) Show that V is a torsion $\mathbb{C}[x]$-module.
(b) Suppose that T has no repeated eigenvalues. Show that V is a cyclic $\mathbb{C}[x]$-module.

12. Let V be a vector space of complex polynomials of degree ≤ 3. Define $T: V \to V$ by

$$T(f(x)) := f(x+1) - f(x).$$

For example, $T(x^2 + x + 2) = ((x+1)^2 + (x+1) + 2) - (x^2 + x + 2) = 2x + 2$. Let $B := \{ 1, x, x(x-1), x(x-1)(x-2) \}$.
(a) Show that B is a basis for V.
(b) Find the matrix of T in the basis B.

PROBLEMS FROM EXAM GIVEN AT LOUISIANA STATE UNIVERSITY ON 16 OCTOBER 1993

1. Let $M_2(\mathbb{F}_5)$ be the ring of 2×2 matrices with coefficients in the finite field $\mathbb{F}_5$. Let

$$A = \begin{pmatrix} 0 & 3 \\ 1 & 0 \end{pmatrix}$$

be an element of this ring and define a ring homomorphism $\phi: \mathbb{F}_5[x] \to M_2(\mathbb{F}_5)$ by setting $\phi(f(x)) = f(A)$.
(a) Determine the kernel of ϕ.
(b) Let K be the image of ϕ. Show that K is a subfield of $M_2(\mathbb{F}_5)$. How many elements does K have?

2. Let $\mathbb{F}_7$ be the field with 7 elements. Define

$$G = \left\{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \,\middle|\, a, b \in \mathbb{F}_7;\ b \in \{1, 2, 4\} \right\}.$$

(a) Verify that G is a subgroup of $GL_2(\mathbb{F}_7)$ of order 21.
(b) Find a 7-Sylow subgroup $N < G$. Is N normal in G?
(c) How many 3-Sylow subgroups does G have? List all of them.

3. Let $K \subseteq \mathbb{Z}^3$ be the $\mathbb{Z}$-module generated by $w_1 = (1, 2, 3)$ and $w_2 = (4, 5, 6)$.
(a) Find a $\mathbb{Z}$-basis $\{ v_1, v_2, v_3 \}$ of $\mathbb{Z}^3$ and integers s_1, s_2 so that $\{ s_1 v_1, s_2 v_2 \}$ is a $\mathbb{Z}$-basis of K.
(b) Find the structure of the finitely generated abelian group $\mathbb{Z}^3/K$; that is, write $\mathbb{Z}^3/K$ as a direct sum of cyclic groups.

4. Let G be a finite group of order 30. Let H be a 5-Sylow subgroup and let K be a 3-Sylow subgroup of G. Show that either H or K is normal in G.

5. Let G be a finite group and let Z be its center.
(a) Show that if G/Z is cyclic, then G is abelian.
(b) Show that if $|G| = p^3$ (p prime) and if G is non-abelian, then $|Z| = p$. (Recall that p-groups have non-trivial center; you may assume this fact.)

6. Let $f(x) = x^3 + x^2 - 2x - 1$.
(a) Show that $f(x)$ is irreducible in $\mathbb{Q}[x]$.
(b) Let $\alpha \in \mathbb{C}$ be a root of $f(x)$. Show that $\alpha^2 - 2$ is also a root of $f(x)$.
(c) Let $K = \mathbb{Q}(\alpha)$. Show that $K/\mathbb{Q}$ is a normal extension and determine its Galois group.

7. Let R be a commutative ring with identity and let $I \subseteq R$ be an ideal. The **radical** of I, denoted $\sqrt{I}$, is defined by

$$\sqrt{I} = \{\, a \in R \mid a^n \in I \text{ for some natural number } n \,\}.$$

(a) Verify that $\sqrt{I}$ is an ideal of R.
(b) Show that $\sqrt{I}$ is contained in the intersection of all prime ideals of R containing I.
(c) If $R = \mathbb{Z}$ and $I = 72\mathbb{Z}$, compute $\sqrt{I}$.

8. Prove that the matrix equation

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

in $M_2(\mathbb{C})$ is not solvable.

9. Let R be a commutative ring with identity and let $f\colon M \to N$ be a surjective map of R-modules.
(a) If R is a field, show $M \cong N \oplus \textsc{Ker}(f)$.
(b) If $R = \mathbb{Z}$, give an example to show that M need not be isomorphic to $N \oplus \textsc{Ker}(f)$.

10. Let $\mathbb{F}_{p^n}$ be the field with p^n elements (p prime). For $\alpha \in \mathbb{F}_{p^n}$ we define

$$T(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + \cdots + \alpha^{p^{n-1}}.$$

Show that $T(\alpha)$ lies in $\mathbb{F}_p$ for all $\alpha \in \mathbb{F}_{p^n}$ and that T defines an $\mathbb{F}_p$-linear map $F_{p^n} \to \mathbb{F}_p$.

11. Let $V = \mathbb{C}^3$ and consider the endomorphism of V given by the matrix

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

relative to the standard basis of V. Find the Jordan normal form of A.

12. Do the following.
(a) Show that any matrix $A \in M_n(\mathbb{C})$ such that $A^k = I$ for some integer $k \geq 1$ is diagonalizable.
(b) Show that (a) need not be true if the complex numbers $\mathbb{C}$ are replaced by an algebraically closed field F of characteristic $p > 0$. (Hint: Check that the matrix

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in M_2(F)$$

satisfies $A^p = I$.)

SAMPLE PROBLEMS FROM UNIVERSITY OF ARIZONA

1. State whether each statement below is true or false.

(a) The row space and the column space of a matrix have trivial intersection.

(b) If $W \subseteq V$ is a subspace of the vector space V, and if $\{ b_1, b_2, \ldots, b_n \}$ is a basis for V, then some subset of $\{ b_1, b_2, \ldots, b_n \}$ is a basis for W.

(c) For every orthogonal matrix M on $\mathbb{R}^n$, there is an orthonormal basis $\{ v_1, v_2, \ldots, v_n \}$ of eigenvectors for M.

(d) If Q is an $n \times n$ orthogonal matrix, then so is Q^{T} (the transpose of Q).

SOLUTION:

(a) False. For example, the row space and the column space of an invertible matrix are each the entire space.

(b) False. For example, there are lots of subspaces of $\mathbb{R}^2$ (such as the line $y = x$) whose basis is disjoint from the canonical $\mathbb{R}^2$ basis.

(c) False. A real matrix is orthogonal if and only if its columns (equivalently, its rows) form an orthonormal basis. The real symmetric matrices are precisely the matrices that can be diagonalized by real orthogonal matrices; the columns of the orthogonal matrix are the eigenvectors of the symmetric matrix. Thus for every real symmetric matrix, there is an orthonormal basis of its eigenvectors. Conversely, if there is an orthonormal basis of eigenvectors of a real matrix M, then the matrix M is diagonalizable; the diagonalizing matrix consists of the eigenvectors and thus is orthogonal; therefore M can be orthogonally diagonalized, and therefore M is symmetric. Since there exist orthogonal matrices that are not symmetric, the statement is false.

(d) True. By definition, Q is orthogonal if and only if $QQ^{\mathrm{T}} = Q^{\mathrm{T}}Q = I$. Clearly Q is orthogonal if and only if Q^{T} is orthogonal.

2. Let V_1 and V_2 denote two vector spaces of equal finite dimension. Show that a linear transformation $f\colon V_1 \to V_2$ is one-to-one if and only if it is onto.

SOLUTION:

Note that the behavior of f is characterized by its behavior on a basis of V_1. In any vector space, a basis is a linearly independent spanning set. In a vector space of dimension n (finite), any set of n linearly independent vectors forms a basis, and any spanning set of n vectors forms a basis. (Both statements fail in infinite dimensions.) I will show that f is one-to-one if and only if f carries a basis to a basis. I will also show that f is onto if and only if f carries a basis to a basis. Clearly, the result to be shown then follows.

Let $\{ v_1, v_2, \ldots, v_n \}$ be a basis of V_1. Let f be one-to-one. Then $\textsc{Ker}(f) = \{0\}$. I claim that the set $\{ fv_1, fv_2, \ldots, fv_n \}$ is linearly independent (and thus, since it must contain n elements, is a basis). Let $a_1 fv_1 + \cdots + a_n fv_n = 0$; then $f(a_1 v_1 + \cdots + a_n v_n) = 0$; thus $a_1 v_1 + \cdots + a_n v_n = 0$; and thus $a_1 = \cdots = a_n = 0$. Therefore f carries a basis to a basis. On the other hand, if f carries a basis to a basis, then if $f \sum_{a_i v_i} = f \sum_{b_i v_i}$, then $\sum_{a_i f v_i} = \sum_{b_i f v_i}$, thus $a_i = b_i$ (since the fv_i form a basis), and thus f is one-to-one.

Let f be onto. Then the set $\{ fv_1, fv_2, \ldots, fv_n \}$, which consists of at most n elements, is a spanning set of an n-dimensional space. Since you need at least n vectors to span, the set consists of exactly n elements and is a basis. On the other hand, if f carries a basis to a basis, then f is clearly onto.

3. Find an orthonormal basis for $\mathbb{R}^2$ with respect to which

$$A = \begin{bmatrix} 4 & 1 \\ 1 & 2 \end{bmatrix}$$

is represented by a diagonal matrix.

SOLUTION:

The real symmetric matrices are precisely the matrices that can be orthogonally diagonalized (that is, can be diagonalized by real orthogonal matrices). The characteristic polynomial of A is

$$(4-\lambda)(2-\lambda)-1=\lambda^2-6\lambda+7.$$

The roots of this polynomial (and thus the eigenvalues of A) are $\lambda = 3\pm\sqrt{2}$. The eigenspace corresponding to the eigenvalue $3+\sqrt{2}$ consists of all vectors (x,y) that are solutions to $(1-\sqrt{2})x+y=0$; that is, all vectors of the form $\big(t,-(1-\sqrt{2})t\big)$. The eigenspace corresponding to the eigenvalue $3-\sqrt{2}$ consists of all vectors (x,y) that are solutions to $(1+\sqrt{2})x+y=0$; that is, all vectors of the form $\big(t,-(1+\sqrt{2})t\big)$. Nonzero representative vectors from each space are $(1,-1+\sqrt{2})$ and $(1,-1-\sqrt{2})$. The length of the former is $\sqrt{4-2\sqrt{2}}$; the length of the latter is $\sqrt{4+2\sqrt{2}}$. Thus the orthogonal matrix

$$P=\begin{bmatrix} \frac{1}{\sqrt{4-2\sqrt{2}}} & \frac{1}{\sqrt{4+2\sqrt{2}}} \\ \frac{1}{\sqrt{4-2\sqrt{2}}}(-1+\sqrt{2}) & \frac{1}{\sqrt{4+2\sqrt{2}}}(-1-\sqrt{2}) \end{bmatrix}$$

diagonalizes A. The problem statement asks for an orthonormal basis with respect to which A is diagonal; this makes no sense. One does not represent a matrix with respect to a basis; one represents linear transformations as a matrix, and that representation depends on a coordinate system given by a basis. Perhaps the intended meaning is that I am to view A as a linear transformation given to me by its representing matrix with respect to the canonical $\mathbb{R}^2$ basis; then I am being asked to find an orthonormal basis with respect to which the matrix representing the linear transformation A will be diagonal. Well, that basis will either be the two columns of P or perhaps the two columns of P^{-1}. Things go one way with representing matrices and the opposite way with linear transformations, and at this point I am a bit confused what type of object A is.

---

4. Show by example that every group of order 4 can occur as a Galois group over some field (you may choose the field).

SOLUTION:

There are precisely two groups of order 4, namely the cyclic group of order 4 (a concrete group with that structure is the underlying additive group of the ring $\mathbb{Z}/4\mathbb{Z}$) and the Klein 4-group (a concrete group with that structure is the underlying additive group of the ring $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$).

Let ζ be a fifth root of unity; that is, let ζ be a nontrivial solution of $x^5=1$; that is, let ζ be a root of the polynomial $x^4+x^3+x^2+x+1$. The Galois group of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$ is cyclic of order 4.

The Galois group of $\mathbb{Q}(\sqrt{2},\sqrt{3})$ is the Klein 4-group.

[Perhaps we weren't supposed to choose the field. Perhaps we were supposed to show, for any given field, that either group can occur. I modified the original problem statement but it seemed too easy now.]

---

5. Give an example of two nonzero modules M,N over a ring R such that

$$M\otimes_R N=\{0\};$$

justify your answer.

SOLUTION:

Let the ring have zero divisors; for example, let $R=\mathbb{Z}/8\mathbb{Z}$, so that $2,4$ are zero divisors. Then $M=N=\mathbb{Q}$ are modules over R. However, any $m\otimes n=(a/b)\otimes(c/d)=(4a/4b)\otimes(2c/2d)=4(a/4b)\otimes 2(c/2d)=0$. **[IS $\mathbb{Q}$ REALLY A MODULE OVER R? MAKE SURE!]**

---

6. Give an example of a prime ideal in $\mathbb{C}[x,y]$.

SOLUTION:

A prime ideal is $\mathfrak{p}=(x)$; this ideal consists of those polynomials in x,y that have an x in every term. If a product of two polynomials is of this form, then at least one of the factors must have this form; else, if both factors have some term with no x, then the product of these terms has no x and appears in the big product polynomial. The ideal (y) is also prime; neither ideal is maximal; both are contained in the maximal (hence also prime) ideal (x,y).

---

7. Let a finite group G act on a finite set X where the cardinality of X is a prime number. Choose $x \in X$ and let $H \leq G$ be the stabilizer of x. Is it true that H is normal in G? Prove or give a counter-example.

SOLUTION:

Here is a counter-example. Let the dihedral group $D_{2\times 3}$ act on the vertices of an equilateral triangle; color the vertices in pink, orange on white polka dot, and rainbow; then label the vertices R, G, and B. Focus your attention on the vertex R. Its stabilizer is the subgroup of order 2 consisting of the identity element and the transposition (GB). This subgroup is not normal; for example, $(RGB)(GB)(RBG) = (RB)$.

---

8. Let p be a prime number. Let $\mathbb{F}_p$ be the field of p elements. Let $G = GL_2(\mathbb{F}_p)$ be the 2×2 invertible matrices with entries in $\mathbb{F}_p$. Let G act on $V = \mathbb{F}_p \times \mathbb{F}_p$ in the usual way (by matrix multiplication).
(a) Show that G has exactly 2 orbits on V.
(b) Compute the order of the stabilizer of $(1, 0)$.
(c) Use part (b) to compute the order of G.

SOLUTION:

(a) The element $(0, 0) \in V$ composes one orbit; certainly $A0 = 0$ for any matrix A, and if $Ax = 0$ for an invertible matrix A, then $x = A^{-1}0 = 0$. I shall now show that the rest of V composes the second orbit. To establish this, I must show, given any nonzero $x, y \in V$, the existence of an invertible matrix A such that $Ax = y$. If x, y are linearly dependent then $\lambda x = y$ and thus the matrix $A = \lambda I$ will serve well. Else, if x, y are linearly independent, then [**I don't know what to do**].

(b) The index of the stabilizier of $(1, 0)$ is the size of the orbit of $(1, 0)$; the order of V is p^2; thus the size of the orbit of $(1, 0)$ is $p^2 - 1$; the order of the stabilizer of $(1, 0)$ is the order of G divided by $p^2 - 1$. But I don't know the order of G; from the question in part (c) I guess that I am not supposed to know this order yet; I conclude that I am supposed to compute the order of the stabilizer more directly. Let

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}.$$

Then $a = 1$ and $c = 0$; the entries b, d are arbitrary subject to the condition $ad - bc \neq 0$; that condition now is merely $d \neq 0$; thus there are p choices for b and $p - 1$ choices for d; this gives $p(p - 1)$ choices for the matrix and thus this is the order of the stabilizer.

(c) From the comments in part (b), the order of the stabilizer of $(1, 0)$, namely $p(p - 1)$, is the order of G divided by $p^2 - 1$, the index of that stabilizer; thus the order of G is $p(p - 1)^2(p + 1) = (p^2 - 1)(p^2 - p) = p^4 - p^3 - p^2 + p$; the answer isn't pretty but so it goes.

---

9. Let R be a ring and suppose that M_1, M_2, and M_3 are three left R-modules. Let $f\colon M_1 \to M_2$ be a homomorphism.
(a) Show that f induces a homomorphism

$$g\colon \mathrm{Hom}_R(M_2, M_3) \to \mathrm{Hom}_R(M_1, M_3).$$

(b) Show that if f iss urjective, then g is injective.
(c) If f is injective, is g surjective? Give a proof or a counter-example.

---

10. State a complete structure theorem for finitely generated modules over the ring $\mathbb{C}[x]/(x^3 - 1)$. Note that this ring is not a PID; it is not even a domain.

---

11. Let P be the polynomial $P(x) = x^3 - 2$. For each field K from the list $\mathbb{Q}$, $\mathbb{F}_3$, $\mathbb{F}_5$, $\mathbb{F}_7$, $\mathbb{Q}(e^{2\pi i/3})$, let E be the field obtained by adjoining a single root of P to K, and let F be the splitting field of P.
(a) Find the degrees of E/K and F/K.
(b) Decide which of the extensions E/K, F/K, and F/E are Galois.
(c) For those extensions that are Galois, compute the Galois group.

PROBLEMS FROM EXAM GIVEN AT UNIVERSITY OF ARIZONA IN JANUARY 1996 (GROVE AND KIM)

1. Let V be a vector space of dimension n over $\mathbb{R}$, and let $0 = V_0 \subseteq V_1 \subseteq \cdots \subseteq V_{n-1} \subseteq V_n = V$ be a sequence of subspaces with $\operatorname{DIM}(V_i) = i$. Define a group G by

$$G = \left\{ g \in \mathrm{GL}(V) \;\middle|\; gV_i \subseteq V_i \text{ for all } i \right\}.$$

Give as complete a description as possible of the structure of G.

2. Show that every 2×2 real matrix with all entries positive can be diagonalized (over $\mathbb{R}$).

3. Find all groups of order 33.

4. Either give an example of a finite group having its center of prime index or prove that such a group cannot exist.

5. The ring $R = \mathbb{Q}[x]/\langle x^4 - 16\rangle$ is a direct sum of fields. Describe the fields explicitly and determine how many of each appear as direct summands.

SOLUTION:

In $\mathbb{Q}[x]$, the principal ideal generated by $x^4 - 16 = (x-2)(x+2)(x^2+4)$ is the same as the product of the principal ideals generated by each irreducible factor. By the Chinese remainder theorem,

$$\frac{\mathbb{Q}[x]}{\langle x-2\rangle\langle x+2\rangle\langle x^2+4\rangle} \cong \frac{\mathbb{Q}[x]}{\langle x-2\rangle} \oplus \frac{\mathbb{Q}[x]}{\langle x+2\rangle} \oplus \frac{\mathbb{Q}[x]}{\langle x^2+4\rangle}.$$

Now $\mathbb{Q}[x]$ is a UFD, hence irreducible elements are prime, and in general, prime elements generate principal prime ideals. Furthermore $\mathbb{Q}[x]$ is a PID, hence nonzero prime ideals are maximal, and thus each of the terms in the direct sum consists of $\mathbb{Q}[x]$ modulo a maximal ideal; that is, each term is a field. Each such field contains a copy of $\mathbb{Q}$, and thus may be viewed as a vector space over $\mathbb{Q}$; as such, the dimension (also called degree) over $\mathbb{Q}$ is the same as the degree of the polynomial that generated the corresponding maximal ideal. In particular, the first two fields in the direct sum displayed above are degree 1 extensions of $\mathbb{Q}$, while the last field is a degree 2 extension of $\mathbb{Q}$, isomorphic to the complex subfield $\mathbb{Q}(i)$, where $i = \sqrt{-1}$. To answer the question, the original ring R is a direct sum of three fields, two of them isomorphic to $\mathbb{Q}$, the last isomorphic to $\mathbb{Q}(i)$.

6. Give a proof or counterexample: Every UFD is a PID.

7. Give an explicit example (with justification) of an irreducible polynomial of degree 100 in $\mathbb{C}[x, y]$.

8. Find the Galois group over $\mathbb{Q}$ of $f(x) = x^5 - 80x + 2$. (Hint: How many real roots does $f(x)$ have?)

SOLUTION:

Note first that f is Eisenstein and hence irreducible over $\mathbb{Q}$. Being of odd degree, f has at least one real root. A quick analysis of $f'(x) = 5x^4 - 80 = 5(x-2)(x+2)(x^2+4)$ shows that f has critical values $x = \pm 2$, and in fact the point $(-2, 130)$ is a local maximum while the point $(2, -126)$ is a local minimum. Hence f has three real roots, and a pair of complex conjugate roots.

The Galois group G of the splitting field of f over $\mathbb{Q}$ may be viewed as acting on the roots of f; viewed in this fashion, G is a transitive permutation group of a set of five elements, and thus is isomorphic to some transitive subgroup of S_5. Viewing the splitting field K of f as a subfield of $\mathbb{C}$, complex conjugation is certainly an automorphism of $\mathbb{C}$ that fixes $\mathbb{Q}$ pointwise, and thus is also an automorphism of K that fixes $\mathbb{Q}$ pointwise; furthermore, the presence of imaginary roots shows K not to be a subfield of $\mathbb{R}$, and thus complex conjugation is a nontrivial $\mathbb{Q}$–automorphism of K. From the viewpoint of root permutations, the complex conjugation automorphism fixes three roots and swaps two roots; hence, when viewed as a subgroup of S_5, the group G contains a transposition.

Since some but not all roots are real, adjoining one root (say, a real one) to $\mathbb{Q}$ cannot split f; at least a quadratic factor remains, and thus the splitting field K has degree at least 10 over $\mathbb{Q}$.

[SO WHY IS THERE A 5-CYCLE?]

---

9. Let $f(x) = x^4 + 5x^2 + 9 \in \mathbb{Q}[x]$. Is $f(x)$ irreducible? Determine its Galois group over $\mathbb{Q}$.

SOLUTION:

Let α be a root of f; that is, $f(\alpha) = 0$, and the quadratic formula gives

$$\alpha^2 = \frac{-5 \pm \sqrt{-11}}{2}.$$

Hence the factorization of f in its splitting field may be expressed in radicals as

$$\begin{aligned} f(x) &= \left(x^2 + \tfrac{1}{2}(5 + \sqrt{-11})\right)\left(x^2 + \tfrac{1}{2}(5 - \sqrt{-11})\right) \\ &= \left(x - i\sqrt{\tfrac{1}{2}(5 + \sqrt{-11})}\right)\left(x + i\sqrt{\tfrac{1}{2}(5 + \sqrt{-11})}\right)\left(x - i\sqrt{\tfrac{1}{2}(5 - \sqrt{-11})}\right)\left(x + i\sqrt{\tfrac{1}{2}(5 - \sqrt{-11})}\right). \end{aligned}$$

Note that I have not yet determined whether f is irreducible. Evidently f has no roots in $\mathbb{Q}$, so that the only possible factorization over $\mathbb{Q}$ is into a pair of quadratic factors. By combining the linear factors (over the splitting field), other factorization of f into a pair of quadratic factors may be obtained. If none of those factorizations lives over $\mathbb{Q}$, then f will have been shown to be irreducible over $\mathbb{Q}$. The product of the first and last linear factors is a quadratic polynomial whose constant term is

$$\sqrt{\tfrac{1}{4}(25 + 11)} = \sqrt{9} = 3$$

and whose degree 1 term has coefficient

$$i\sqrt{\tfrac{1}{2}(5 - \sqrt{-11})} - i\sqrt{\tfrac{1}{2}(5 + \sqrt{-11})}.$$

I question whether the latter lives in $\mathbb{Q}$. Squaring it gives

$$-\tfrac{1}{2}(5 - \sqrt{-11}) - 3 - \tfrac{1}{2}(5 + \sqrt{-11}) = FUCK,$$

which, of course, is a square in $\mathbb{Q}$. Hence f is reducible after all, having $x^2 + x + 3$ or $x^2 - x + 3$ as a root! In fact, the factorization of f into irreducibles over $\mathbb{Q}$ is $f(x) = (x^2 + x + 3)(x^2 - x + 3)$. Although my previous work seems to indicate that f splits completely in $\mathbb{Q}(\sqrt{-11})$, this fact is confirmed by observing that each quadratic factor has discriminant -11. Hence the splitting field of f is the degree 2 extension $\mathbb{Q}(\sqrt{-11})/\mathbb{Q}$, and the Galois group is cyclic of order 2.

---

10. Give a proof or counterexample: Every finitely generated torsion-free module over a discrete valuation ring is free.

---

11. Let A be the abelian group with presentation

$$A = \left\langle a, b, c \;\middle|\; 2a + 4b + 2c = 0,\ 2a + 10b + 8c = 0 \right\rangle.$$

Determine the order and the structure of the torsion subgroup T (the subgroup of elements of finite order) of A.

PROBLEMS FROM EXAM GIVEN AT UNIVERSITY OF ARIZONA IN AUGUST 1995 (MCCALLUM AND ULMER)

---

1. Find all eigenvalues and eigenvectors of M and of M^{100}, where

$$M = \begin{bmatrix} -12 & 18 \\ -8 & 12 \end{bmatrix}.$$

SOLUTION:

Recall that an eigenvalue of M is any number λ so that there exists a nonzero column vector $\mathbf{v}$ with $M\mathbf{v} = \lambda\mathbf{v}$. The latter is equivalent to $(M - \lambda I)\mathbf{v} = \mathbf{0}$, and, to a given value of λ, a nonzero solution $\mathbf{v}$ exists precisely when the matrix $M - \lambda I$ is singular, i.e., when $\operatorname{DET}(M - \lambda I) = 0$. The latter equation is equivalent to $\lambda^2 = 0$, so that 0, with algebraic multiplicity 2, is the unique eigenvalue of M. The eigenspace corresponding to the eigenvalue 0 consists of all vectors (including $\mathbf{0}$) that satisfy $M\mathbf{v} = \mathbf{0}$; that space of vectors is precisely the null space of M. Since the null space does not change under row operations, I may row reduce M to obtain

$$\begin{bmatrix} 2 & -3 \\ 0 & 0 \end{bmatrix},$$

and I see that the null space is 1–dimensional, spanned by the vector $(3, 2)$. In other words, every eigenvector of M is some scalar multiple of $(3, 2)$.

Since the characteristic polynomial of M is X^2, I see that $M^{100} = 0$, so that M^{100} has the eigenvalue 0 with algebraic multiplicity 2, and every vector is an eigenvector of M^{100}.

---

2. Let V be a finite dimensional vector space over a field $\mathbb{F}$, and let $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{F}$ be a bilinear form. Prove that the spaces

$$\{\, v \in V \mid \langle v, w \rangle = 0 \text{ for all } w \in V \,\} \quad \text{and} \quad \{\, w \in V \mid \langle v, w \rangle = 0 \text{ for all } v \in V \,\}$$

have the same dimension.

SOLUTION:

By fixing the first coordinate $\mathbf{v}$, the bilinear form $\langle \mathbf{v}, \cdot \rangle$ becomes a linear functional, i.e., $\langle \mathbf{v}, \cdot \rangle \in \operatorname{HOM}(V, \mathbb{F})$. Thus I have a map $\phi: V \to \operatorname{HOM}(V, \mathbb{F})$ given by $\phi(\mathbf{v}) = \langle \mathbf{v}, \cdot \rangle$. Similarly, I have a map $\psi: V \to \operatorname{HOM}(V, \mathbb{F})$ given by $\psi(\mathbf{w}) = \langle \cdot, \mathbf{w} \rangle$. The two spaces given in the problem statement are merely the kernels of these maps; thus I wish to prove that $\operatorname{DIM}(\operatorname{KER} \phi) = \operatorname{DIM}(\operatorname{KER} \psi)$. To do this, I will reformulate the problem in the language of matrices.

Let $\{\, \mathbf{e}_1, \ldots, \mathbf{e}_n \,\}$ be a basis of V. Let M denote the $n \times n$ matrix whose entries are given by $\langle \mathbf{e}_i, \mathbf{e}_j \rangle$. If the coordinate vector of $\mathbf{v}$ is $(v_1, \ldots, v_n)$ and the coordinate vector of $\mathbf{w}$ is $(w_1, \ldots, w_n)$, then $\langle \mathbf{v}, \mathbf{w} \rangle$ may be computed as

$$\begin{bmatrix} v_1 & \cdots & v_n \end{bmatrix} M \begin{bmatrix} w_1 \\ \vdots \\ w_n \end{bmatrix},$$

which I shall abbreviate as $[\mathbf{v}]^{\mathrm{T}} M [\mathbf{w}]$.

Asking whether $\phi(\mathbf{v}) = \langle \mathbf{v}, \cdot \rangle$ is the zero functional is the same as asking whether $[\mathbf{v}]^{\mathrm{T}} M$ is the zero row vector. Transposing gives me the equation $M^{\mathrm{T}}[\mathbf{v}] = 0$, and so I see that $\operatorname{DIM}(\operatorname{KER} \phi)$ is just the nullity of M^{T}.

Asking whether $\psi(\mathbf{w}) = \langle \cdot, \mathbf{w} \rangle$ is the zero functional is the same as asking whether $M[\mathbf{w}]$ is the zero column vector. Thus $\operatorname{DIM}(\operatorname{KER} \psi)$ is just the nullity of M.

Since a matrix and its transpose have the same nullity, I conclude that $\operatorname{DIM}(\operatorname{KER} \phi) = \operatorname{DIM}(\operatorname{KER} \psi)$, as desired.

---

3. Is it possible for the symmetric group S_4 to act transitively on a set with 3 elements? Justify your answer completely.

SOLUTION:

The answer is yes; an explicit example is given below. In any group action, the index of the stabilizer (of a point in a particular orbit) is the same as the size of the orbit. A transitive action has a single orbit, which in this case consists of three points. Thus the stabilizer of each point has index 3; since S_4 has $24 = 2^3 \cdot 3$ elements, each stabilizer has order 8. Since 8 is the highest power of 2 that divides the order of S_4, any 2–Sylow subgroup of S_4 has order 8; furthermore, the Sylow theorems guarantee the existence of at least one such subgroup. (In fact, the Sylow theorems tell me that either there is 1 or there are 3 such subgroups, but the exact number is unimportant at present.) Let H denote one of those subgroups. The set G/H of left cosets is not necessarily a group (namely, if there are three 2–Sylow subgroups, then H is not normal), but nevertheless G acts on that left coset space by left translation. This action is immediately seen to be transitive, as the group element ba^{-1} moves the coset aH to the coset bH.

4. Let $\mathrm{GL}_n(\mathbb{R})$ be the group of invertible $n \times n$ matrices with real coefficients. Let V be the vector space $\mathbb{R}^3$ of column vectors, and let $\mathrm{GL}_3(\mathbb{R})$ act by linear transformation on V. Let $G \subseteq \mathrm{GL}_n(\mathbb{R})$ be the subgroup of matrices that preserve the subspace V_0, where V_0 comprises the vectors whose last entry is zero. Prove that there exists a normal subgroup $H \subseteq G$ such that G/H is isomorphic to $\mathrm{GL}_2(\mathbb{R})$. Describe H explicitly.

SOLUTION:

The matrices that fix V_0 are precisely the ones of the form

$$\begin{bmatrix} * & * & * \\ * & * & * \\ 0 & 0 & * \end{bmatrix},$$

where the entries along the diagonal are nonzero. Let H comprise those matrices in G whose upper-left 2×2 submatrix is the 2×2 identity matrix; note that the bottom-right entry in any matrix in H is nonzero. As the inverse of the matrix

$$\begin{bmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & c \end{bmatrix}$$

is the matrix

$$\begin{bmatrix} 1 & 0 & -a/c \\ 0 & 1 & -b/c \\ 0 & 0 & 1/c \end{bmatrix},$$

the subset $H \subseteq G$ is quickly seen to be a subgroup of G.

Consider the map $\phi\colon G \to \mathrm{GL}_2(\mathbb{R})$ that throws away the bottom row and last column; it is most easily seen to be a group homomorphism by partitioning each matrix of G to form a block matrix whose upper-left block is 2×2. Then

$$\begin{bmatrix} A & B \\ 0 & D \end{bmatrix}\begin{bmatrix} E & F \\ 0 & G \end{bmatrix} = \begin{bmatrix} AE & AF+BG \\ 0 & DG \end{bmatrix},$$

so that

$$\phi\begin{bmatrix} AE & AF+BG \\ 0 & DG \end{bmatrix} = AE = \phi\begin{bmatrix} A & B \\ 0 & D \end{bmatrix}\phi\begin{bmatrix} E & F \\ 0 & G \end{bmatrix}.$$

Since H is obviously the kernel of this map, H must be normal in G. Furthermore, the map is clearly surjective. Therefore, the fundamental homomorphism theorem tells me that G/H is isomorphic to $\mathrm{GL}_2(\mathbb{R})$.

---

5. Give an example of an ideal in a commutative ring that is prime but not maximal.

SOLUTION:

Let the ring be $\mathbb{Z}[X]$. Since 2 is a prime element of the ring, the principal ideal $\langle 2\rangle$ is a prime ideal. However, since $\langle 2\rangle$ is properly contained in $\langle 2, X\rangle$, and the latter is not the entire ring, the ideal $\langle 2\rangle$ is not maximal.

---

6. Let $f\colon R \to S$ be a homomorphism of commutative rings. Prove that if $I \subset S$ is a prime ideal, then $f^{-1}(I)$ is also a prime ideal. Give an example where I is maximal but $f^{-1}(I)$ is not maximal.

SOLUTION:

I shall first show that the preimage under f of *any* ideal in S is an ideal in R. Let I be an ideal in S. Since $f(0) = 0$, certainly $f^{-1}(I)$ is nonempty. If $a, b \in f^{-1}(I)$, then $f(a-b) = f(a) - f(b) \in I$, so that $a - b \in f^{-1}(I)$. Therefore $f^{-1}(I)$ is an additive subgroup of R. Finally, if $r \in R$ and $a \in f^{-1}(I)$, then $f(ra) = f(r)f(a) \in I$, so that $ra \in f^{-1}(I)$. Therefore $f^{-1}(I)$ is an ideal of R.

Now let I be prime. Let $ab \in f^{-1}(I)$. Then $f(ab) = f(a)f(b) \in I$, so that either $f(a) \in I$ or $f(b) \in I$, and thus either $a \in f^{-1}(I)$ or $b \in f^{-1}(I)$. Therefore $f^{-1}(I)$ is seen to be prime.

For an example where I is maximal but $f^{-1}(I)$ is not maximal, let me first note the following. If $f\colon R \to S$ is surjective, then $f^{-1}(I)$ *is* maximal whenever I is. Furthermore, in any PID all nonzero prime ideals are maximal, and if the PID is a field, then in fact the zero ideal itself is maximal. Hence, to find an example, I must look where f is not surjective and where R is not a field. A trivial example is the injection $\mathbb{Z} \hookrightarrow \mathbb{Q}$, where the preimage of the zero ideal (maximal in $\mathbb{Q}$) is the zero ideal (not maximal in $\mathbb{Z}$). A more interesting example is obtained when R is not even a PID. For example, consider the injection $\mathbb{Z}[X] \hookrightarrow \mathbb{Q}[X]$; now the preimage of the maximal ideal $\langle X\rangle \subset \mathbb{Q}[X]$ is the ideal $\langle X\rangle \subset \mathbb{Z}[X]$, which is properly contained in the maximal ideal $\langle 2, X\rangle \subset \mathbb{Z}[X]$.

7. Does there exist a ring R with 10 elements such that whenever $a \neq 0$ and $b \neq 0$, then also $ab \neq 0$? Justify your answer completely.

SOLUTION:

Any finite ring without zero divisors is necessarily either the zero ring or a field; this follows by starting with the easily proved fact that any finite ring without zero divisors necessarily is a division ring (in particular, it necessarily has multiplicative identity) and then applying Wedderburn's theorem, which says that each finite division ring is commutative (whence a field). But there is no field with 10 elements. Hence the answer to the problem is "no".

Here is a more direct proof that does not make use of Wedderburn's theorem. The additive structure of R is an abelian group on 10 elements, and $\mathbb{Z}/10\mathbb{Z}$ is the only such group. Hence, I shall label the elements of R as $\{0, 1, 2, \ldots, 9\}$, keeping in mind that the multiplication might be weird. Apply distributive properties to calculate $2 \cdot 5 = (1+1) \cdot (1+1+1+1+1) = 1 \cdot (1+1+1+1+1) + 1 \cdot (1+1+1+1+1) = 1 \cdot 1 + \ldots + 1 \cdot 1$, where there are ten copies of $1 \cdot 1$ at the end. Now $1 \cdot 1$ is *some* element of the group $\mathbb{Z}/10\mathbb{Z}$, thus adding up 10 copies always gives 0. Hence R necessarily has zero divisors.

8. Let $E \subseteq F \subseteq L$ be three fields. Prove or give a counterexample to the following statements:

- L is Galois over E implies that L is Galois over F and F is Galois over E.
- L is Galois over F and F is Galois over E implies that L is Galois over E.

SOLUTION:

The first statement is false. If L is Galois over E, then L is also Galois over F, but then F is Galois over E if and only if F is normal over E. Here is an example: $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(e^{2\pi i/3}, \sqrt[3]{2})$. The latter is the splitting field of $X^3 - 2$ over $\mathbb{Q}$. One of the embeddings into $\mathbb{C}$ sends $\mathbb{Q}(\sqrt[3]{2})$ to its isomorphic brother $\mathbb{Q}(e^{2\pi i/3}\sqrt[3]{2})$, which does not fix $\mathbb{Q}(\sqrt[3]{2})$ as a set, since $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$, while $\mathbb{Q}(e^{2\pi i/3}\sqrt[3]{2})$ contains imaginary numbers; thus $\mathbb{Q}(\sqrt[3]{2})$ is not normal over $\mathbb{Q}$.

The second statement is false. Here is an example: $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$. Each intermediate extension has degree 2 and is forced to be Galois, while the full extension cannot be Galois, for it is not normal: one of the $\mathbb{Q}$–embeddings of $\mathbb{Q}(\sqrt[4]{2})$ into $\mathbb{C}$ sends $\mathbb{Q}(\sqrt[4]{2})$ to $\mathbb{Q}(i\sqrt[4]{2})$.

9. Let f be a quintic polynomial with coefficients in $\mathbb{Q}$ such that the splitting field K of f has Galois group isomorphic to the dihedral group D_5. Prove that there exists a unique quadratic field $\mathbb{Q}(\sqrt{d}) \subseteq K$, and find an expression for $\sqrt{d}$ in terms of the roots of f.

10. Let R be a commutative Noetherian ring.

- Suppose $\phi\colon M_1 \to M_2$ is a surjective homomorphism of R–modules. Prove that for any R–module N, the homomorphism $\mathrm{Hom}_R(M_2, N) \to \mathrm{Hom}_R(M_1, N)$ induced by composition with ϕ is injective.
- Suppose $\phi\colon N_1 \to N_2$ is a surjective homomorphism of R–modules. Prove that for any *free* R–module F, the homomorphism $\mathrm{Hom}_R(F, N_1) \to \mathrm{Hom}_R(F, N_2)$ induced by composition with ϕ is surjective.
- Use the previous two results to prove that if M and N are finitely generated R–modules, then $\mathrm{Hom}_R(M, N)$ is also finitely generated.

11. Let R be the polynomial ring $\mathbb{C}[T]$, and let M be the vector space of column vectors $\mathbb{C}^3$. Make M into an R–module by letting $\mathbb{C}$ act by scalar multiplication and letting T act by the matrix

$$\begin{bmatrix} 2 & 7 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1+i \end{bmatrix}.$$

Write down a direct sum of cyclic R–modules that is isomorphic to M.

PROBLEMS FROM EXAM GIVEN AT UNIVERSITY OF ARIZONA IN JANUARY 1995 (GROVE AND MCCALLUM)

1. Find an orthogonal matrix that diagonalizes

$$A = \begin{bmatrix} 5 & 12 \\ 12 & -5 \end{bmatrix}.$$

2. Suppose V is a vector space and $T\colon V \to V$ is a linear transformation for which every nonzero vector is an eigenvector. Prove that T is a scalar multiple of the identity transformation.

SOLUTION:

Fix some nonzero vector x; then x is an eigenvector and thus has a corresponding eigenvalue; that is, $Tx = \lambda x$ for some λ. I claim that every nonzero vector in the span of x has the same eigenvalue; after all, $T(cx) = cTx = c\lambda x = \lambda(cx)$. If the dimension of V is 1, then I am done; else any vector in V not in the span of x will be linearly independent of x; I shall now show that such a vector also has λ as its eigenvalue. Fix $y \in V$ not in the span of x; certainly $y \neq 0$; thus y is an eigenvector and has some corresponding eigenvalue, say $Ty = \mu y$. Now certainly $x + y \neq 0$ since x, y are linearly independent. Thus $x + y$ is an eigenvector and therefore $T(x + y) = \nu(x + y)$ for some ν. Then $Tx + Ty = \lambda x + \mu y = \nu x + \nu y$; thus $(\lambda - \nu)x + (\mu - \nu)y = 0$ and linear independence rescues us once more to tell us $\lambda = \nu$ and $\mu = \nu$; even a mere laddy can substitute transitively to get $\lambda = \mu$. Let me summarize. Every nonzero vector in the span of x has the same eigenvalue as x. Every nonzero vector not in the span of x has the same eigenvalue as x. Therefore, every nonzero vector has the same eigenvalue; I'm calling that value λ. Thus for any vector z (including zero), $Tz = \lambda z$; thus T is a scalar multiple (namely by λ) of the identity transformation.

Here is a slightly different solution. My goal is to show that T has a single eigenvalue, i.e., there exists γ such that $Tv = \gamma v$ for all $v \in V$. Assume on the contrary that T has at least two *distinct* eigenvalues, say α_1 and α_2. Let v_1 and v_2 be corresponding eigenvectors. Since the distinctness of the eigenvalues forces v_1 and v_2 to be linearly independent, the new vector $v = v_1 + v_2$ is nonzero, and thus, by the problem statement, v must be an eigenvector, say $Tv = \alpha v$. Thus we can write

$$Tv = \alpha v = \alpha(v_1 + v_2) = \alpha v_1 + \alpha v_2,$$
$$Tv = T(v_1 + v_2) = Tv_1 + Tv_2 = \alpha_1 v_1 + \alpha_2 v_2,$$

and so $\alpha v_1 + \alpha v_2 = \alpha_1 v_1 + \alpha_2 v_2$. Using the linear independence of v_1 and v_2 again, we conclude $\alpha = \alpha_1$ and $\alpha = \alpha_2$, contradicting the distinctness of α_1 and α_2.

3. Suppose p is a prime and G is a finite group. A subgroup K of G is called a **normal p-complement** if $K \triangleleft G$ and there is a Sylow p-subgroup P such that $K \cap P = 1$ and $KP = G$. Show that if G has a normal p-complement, then it is unique. Give an example.

SOLUTION:

Let me start with an example. The cyclic group $\mathbb{Z}/15\mathbb{Z}$ is the internal direct sum of its cyclic subgroups of order 3 and 5; call them K and P. Here K is a normal 3-complement: certainly K is normal (in an abelian group, every subgroup is normal), and there is a Sylow 5-subgroup, namely P, such that $K \cap P = 1$ and KP is the entire group. [Why did I include this? It doesn't even show the full power, since in general we only need a semidirect product.]

[Solution One] I will make use of the "Hall theorems", which are a generalization of the famous "Sylow theorems". One of the Sylow theorems states that if $p^k \mid |G|$ and $\text{GCD}\, p^k, |G|/p^k = 1$, then there exists a subgroup of order p^k. (They go on to give congruences controlling the number of such subgroups, and to state that any two such subgroups are conjugate.) The Hall theorems are almost identical in statement, only do not require a power of a prime: if $m \mid |G|$ and $\text{GCD}\, m, |G|/m = 1$, then there exists a subgroup of order m, and any two such subgroups are conjugate. Assuming this theorem, the present problem is easy to solve. Since $KP = G$ and $K \cap P = 1$, if the p-Sylow subgroup has order p^k, then our p-complement must have order $|G|/p^k$. The Hall theorems assert that any two subgroups of order $|G|/p^k$ are conjugate. Hence, if we know that we have a normal subgroup of that order, it must be unique. (Note: The Hall theorems do not assert the existence of p-complements; they *do* assert the existence of subgroups of the appropriate order, but there is no guarantee that such a subgroup, together with a p-Sylow, will build the group as an internal semidirect sum.)

[Solution Two] Let the p-Sylow subgroup P have order p^k. Since $KP = 1$ and $K \cap P = 1$, we must have $|K| = |G|/p^k$. I claim that K must be the set of elements of G of order not a multiple of p. (This would show K to be unique.) Let H denote that set of elements. Since each element of K has order dividing $|G|/p^k$, certainly $K \subseteq H$. Now consider the canonical projection map $G \to G/K$, observing that G/K is a p-group. Under group homomorphism, the order of the image of an element must divide the order of the original element. But the only possible orders in G/K are 1, p, p^2, and so on. Hence any element of H gets mapped to an element of order 1, i.e., it represents the trivial coset of K, and thus lies in K. In short, $H \subseteq K$. Combining the pieces, we have $K = H$ and thus K is unique.

---

4. Let n be a positive integer and let $M_n(\mathbb{C})$ denote the set of $n \times n$ matrices with complex entries. For $A \in M_n(\mathbb{C})$, denote its determinant by $\mathrm{Det}\,A$. Let

$$\mathrm{GL}_n(\mathbb{C}) = \{\, A \in M_n(\mathbb{C}) \mid \mathrm{Det}\,A \neq 0 \,\},$$

and let

$$\mathrm{SL}_n(\mathbb{C}) = \{\, A \in M_n(\mathbb{C}) \mid \mathrm{Det}\,A = 1 \,\}.$$

Show that $\mathrm{GL}_n(\mathbb{C})$ is a group under matrix multiplication, that $\mathrm{SL}_n(\mathbb{C})$ is a normal subgroup of $\mathrm{GL}_n(\mathbb{C})$, and identify the quotient group $\mathrm{GL}_n(\mathbb{C})/\mathrm{SL}_n(\mathbb{C})$. You may use the basic properties of matrices and determinants without deriving them.

SOLUTION:

A basic property of determinants is that the determinant of a product is the product of the determinants. Thus the determinant of a matrix inverse is the reciprocal of the determinant of the original matrix. Matrices (over a field) with nonzero determinant are invertible; matrix multiplication is associative; since $\mathbb{C}^*$ (the nonzero complex numbers) are closed under multiplication and taking reciprocals, $\mathrm{GL}_n(\mathbb{C})$ is closed under matrix multiplication and taking inverses; in particular, it has an identity, namely the identity matrix; thus it is a group. Certainly $\mathrm{SL}_n(\mathbb{C})$ is nonempty since it contains the identity matrix; if $A, B \in \mathrm{SL}_n(\mathbb{C})$, then also $AB^{-1} \in \mathrm{SL}_n(\mathbb{C})$ since $\mathrm{Det}(AB^{-1}) = \mathrm{Det}(A)/\mathrm{Det}(B) = 1/1 = 1$; thus $\mathrm{SL}_n(\mathbb{C})$ is a subgroup of $\mathrm{GL}_n(\mathbb{C})$. To show that $\mathrm{SL}_n(\mathbb{C})$ is normal in $\mathrm{GL}_n(\mathbb{C})$, I must show that $\mathrm{SL}_n(\mathbb{C})$ is fixed (as a set, not pointwise) under conjugation by matrices in the group. Let $A \in \mathrm{SL}_n(\mathbb{C})$ and $B \in \mathrm{GL}_n(\mathbb{C})$. Then $BAB^{-1} \in \mathrm{SL}_n(\mathbb{C})$ since $\mathrm{Det}(BAB^{-1}) = \mathrm{Det}(B)\mathrm{Det}(A)/\mathrm{Det}(B) = \mathrm{Det}(A) = 1$.

I claim that $\mathrm{GL}_n(\mathbb{C})/\mathrm{SL}_n(\mathbb{C}) \cong \mathbb{C}^*$, where $\mathbb{C}^*$ is the multiplicative group of nonzero complex numbers. First I will show that two matrices represent the same coset if and only if their determinants are equal; let $[A] = [B]$; then $B^{-1}A \in \mathrm{SL}_n(\mathbb{C})$, and thus $1 = \mathrm{Det}(B^{-1}A) = \mathrm{Det}(A)/\mathrm{Det}(B)$, so that $\mathrm{Det}(A) = \mathrm{Det}(B)$; follow the implications in the opposite direction to see that the necessary condition is sufficient. Thus the map $\phi\colon \mathrm{GL}_n(\mathbb{C})/\mathrm{SL}_n(\mathbb{C}) \to \mathbb{C}^*$ defined by $\phi([A]) = \mathrm{Det}(A)$ is well-defined, one-to-one, and onto. To show that it is a group isomorphism, it remains to show that it is a group homomorphism. But this follows from $\phi([A][B]) = \phi([AB]) = \mathrm{Det}(AB) = \mathrm{Det}(A)\mathrm{Det}(B)$. Thus my claim that $\mathrm{GL}_n(\mathbb{C})/\mathrm{SL}_n(\mathbb{C}) \cong \mathbb{C}^*$ has been established.

---

5. Determine the Galois group over $\mathbb{Q}$ of $f(x) = x^5 + 3x^3 - 2x^2 - 6$.

SOLUTION:

The polynomial $f(x)$ factors as $f(x) = (x^3-2)(x^2+3)$; each factor is irreducible over $\mathbb{Q}$; after all, a degree 2 or degree 3 polynomial factors if and only if it splits off a linear factor (that is, if and only if it has a root); the two roots of x^2+3 are the non-rational numbers $\pm\sqrt{-3}$, and the three roots of x^3-2 are the non-rational numbers $\sqrt[3]{2}$, $e^{2\pi i/3}\sqrt[3]{2}$, and $e^{4\pi i/3}\sqrt[3]{2}$. Note that $e^{2\pi i/3} = (-1+i\sqrt{3})/2$.

The splitting field of f is $\mathbb{Q}(e^{2\pi i/3}, \sqrt[3]{2})$. I claim that this is a degree 6 extension over $\mathbb{Q}$. After all, the degree 3 extension $\mathbb{Q}(\sqrt[3]{2})$ is a subfield of the real numbers and thus does not contain $e^{2\pi i/3}$. Going from $\mathbb{Q}(\sqrt[3]{2})$ to the splitting field is a degree 2 extension since the minimal polynomial of $e^{2\pi i/3}$ is x^2+x+1.

The Galois group of f is a group of order 6; there are precisely two groups of order 6, namely the cyclic abelian group $\mathbb{Z}/6\mathbb{Z}$ and the nonabelian group S_3 (which can also be thought of as the dihedral group $D_{2\times 3}$). Since $\mathbb{Q}(\sqrt[3]{2})$ is an intermediate field that is not normal (since it does not contain the conjugates of $\sqrt[3]{2}$), the fundamental theorem of Galois theory says that the Galois group has a subgroup that is not normal; thus the Galois group cannot be abelian. The Galois group of f is S_3.

---

6. Say whether each of the following is true or false. In each case either provide a proof of the statement or provide a counterexample.

(a) Let K be a field of characteristic 0 and let L be an extension of K of degree 2. Then L is Galois over K.

(b) Let K be a field of characteristic 0 and let L be an extension of K of degree 3. Then L is Galois over K.

SOLUTION:

One of the characterizations of a finite extension being Galois is that it is normal and separable. All extensions in characteristic 0 are separable; one of the characterizations of normality is to be the splitting field of one or more polynomials.

(a) True. A degree 2 extension of K is accomplished by adjoining the root of an irreducible degree 2 polynomial; but adjoining one root splits off a linear factor; since the remaining factor is linear, its root must have gotten adjoined as well. Thus we have reached the splitting field of this polynomial. Look at it another way: starting with a degree n polynomial, the maximum degree of the splitting field is $n!$; here we are working with $2!$ and that is just 2.

(b) False. Adjoining $\sqrt[3]{2}$ to $\mathbb{Q}$ gives a degree 3 extension that is not normal and thus not Galois. The splitting field of $x^3 - 2$ over $\mathbb{Q}$ is a degree 6 extension; one can see that adjoining a single root does not bring in the other roots by noting that adjoining the real cube root of 2 gives an extension that is a subfield of the real numbers, but the splitting field is not a subfield of the reals.

---

7. A commutative ring R with 1 is said to be a local ring if it has exactly one maximal ideal $\mathfrak{m}$. Prove that every element of R is either a unit or is an element of $\mathfrak{m}$.

SOLUTION:

By definition, a maximal ideal is a proper ideal. No proper ideal contains a unit, for the only ideal that contains units is the entire ring. Given any non-unit, it generates a proper ideal that is contained in some maximal ideal (I give this argument below); since the only maximal ideal is $\mathfrak{m}$, it must be that the non-unit is in $\mathfrak{m}$.

I wish to argue that any proper ideal is contained in a maximal ideal. The idea of the argument is simple: if an ideal $\mathfrak{a}$ is proper but not maximal, then by definition there exists a proper ideal between $\mathfrak{a}$ and R; if that ideal is not maximal, then repeat the argument; eventually (possibly after infinitely many steps) one should arrive at a maximal ideal. Worries about what *should* happen are addressed by making the argument precise using a variant of the axiom of choice known as "Zorn's Lemma". I shall partially order the set S of all proper ideals between $\mathfrak{a}$ and R by set inclusion. A chain is a subset that is totally ordered by my order. If I show that any chain has an upper bound in S (not necessarily in the chain), then a quick zornication tells me that S has a maximal element. Given a chain $C \subset S$, I claim that $\bigcup_{\mathfrak{b} \in C} \mathfrak{b}$ (clearly an upper bound of C) lies in S; that is, I claim that the union is an ideal properly caught between $\mathfrak{a}$ and R. Given elements a, b in the union, each lies in some ideal, say A and B. By the total ordering, either $A \subseteq B$ or vice versa. Either way, both a, b lie in the same ideal; thus also their difference lies in that ideal and thus the difference lies in the union. The union is an additive group. Given any element a in the union and an arbitrary $r \in R$, certainly a lies in some ideal A and thus $ra \in A$ and thus ra lies in the union. The union absorbs multiplication. Therefore, the union is an ideal. Clearly this union ideal contains $\mathfrak{a}$. I must still show that the union ideal is proper. An ideal is proper if and only if it does not contain a unit. None of the ideals in the union contains a unit; thus the union itself contains no unit. The union ideal is proper. Therefore every chain C has an upper bound. By Zorn's Lemma, the set S has a maximal element. The set S consisted of all proper ideals between $\mathfrak{a}$ and R; a maximal element of S is thus a proper ideal $\mathfrak{m}$ containing $\mathfrak{a}$ such that no other proper ideal lies above $\mathfrak{m}$; that is, $\mathfrak{m} \subset R$ and if $\mathfrak{m} \subseteq \mathfrak{b} \subseteq R$, then either $\mathfrak{m} = \mathfrak{b}$ or $\mathfrak{b} = R$. The ideal $\mathfrak{m}$ is maximal and contains $\mathfrak{a}$. I have shown that every proper ideal is contained in a maximal ideal.

---

8. Say whether each of the following is true or false. In each case either provide a proof of the statement or provide a counterexample.

(a) Let R be a commutative ring with an identity element and let M be a free R-module. Then every submodule of M is free.

(b) Let R be a commutative ring with an identity element and let M be an R-module. Then M is a finite set if and only if it is finitely generated and every element of M is a torsion element.

SOLUTION:

(a) False. Let $R = M = \mathbb{Z}/4\mathbb{Z}$; certainly $M = R^1$ is free. The submodule $2M = \{0, 2\}$ is not free (since its order, being less than the order of R, cannot be a power of the order of R).

(b) False. Let $R = M = \mathbb{Z}/2\mathbb{Z}$. Then M is finite and is finitely generated, but the element $1 \in M$ is not torsion: to be torsion there must be a nonzero ring element that kills 1, but such a ring element does not exist. Notice that M is a finitely generated module over a principal ideal domain; if the ring R was infinite, then the free part of M would be infinite If one requires R to be an integral domain (some authors, to discuss torsion at all, require the ring to be an integral domain in the first place) and further requires $|R| > |M|$ (for example, require R to be infinite), then the result is true. Here is the proof. If M is a finite set, then it is clearly finitely generated (all of M is a generating set). Fix $x \in M$. The submodule $\langle x \rangle = Rx$ is finite; since $|R| > |M|$, there exist two distinct ring elements r, s with $rx = sx$; thus $(r - s)x = 0$ and therefore x is a torsion element. Now assume that M is finitely generated and that every element of M is a torsion element. **[Actually, the result doesn't seem to be true. Even though there are annihilators, they might have infinite index in the ring, and then the module could still be infinite. Is that possible?]**

---

9. Give the exact structure of the abelian group $\mathbb{Z}^3/M\mathbb{Z}^3$, where

$$M = \begin{bmatrix} 0 & 3 & 2 \\ 3 & 2 & 2 \\ 4 & -2 & 5 \end{bmatrix}.$$

---

10. Suppose V is a vector space; let $\{v_1, \ldots, v_n\}$ be a basis for V; let $\{w_1, \ldots, w_n\} \subseteq V$. Show that if $\sum_{i=1}^{n} v_i \otimes w_i = 0$, then $w_1 = \cdots = w_n = 0$.

PROBLEMS FROM EXAM GIVEN AT UNIVERSITY OF ARIZONA IN AUGUST 1994 (GROVE AND ULMER)

---

1. Suppose A is an $n \times n$ complex matrix and $A^k = I$ for some positive integer k. Prove that A can be diagonalized.

---

2. Say whether each of the following statements is true or false. In each case, justify your claim; that is, give either a short proof or a counterexample.

(a) If a matrix A is both Hermitian and unitary then $A = \pm I$.

(b) If V is a finite dimensional vector space and $T\colon V \to V$ is a linear transformation, then $V = \mathrm{IM}(T) \oplus \mathrm{KER}(T)$.

(c) Eigenvalues of orthogonal matrices are real numbers.

SOLUTION:

(a) False. The matrix

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

is both Hermitian and unitary.

(b) False. Let V be the vector space of those polynomials that have degree strictly less than n. The differentiation operator has the constant polynomials as its kernel and has the polynomials of degree strictly less than $n - 1$ as its image. The entire vector space is *not* the direct sum of these two subspaces. Note, however, that the dimension of the vector space, namely n, is the sum of the dimensions of these two subspaces; that's good, since this fact is guaranteed by a theorem.

(c) False. The matrix

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

is orthogonal and has characteristic polynomial x^2+1; its eigenvalues are $\pm i$.

---

3. How many essentially distinct ways can the alternating group A_4 act transitively on a set with 3 elements?

---

4. Let G be a group; let $H \leq G$; let $x^2 \in H$ for all $x \in G$. Show that $H \triangleleft G$ and G/H is abelian. (Hint: Think about $K = \langle\, x^2 : x \in G\,\rangle$).

SOLUTION:

First I claim that any subgroup containing the commutator subgroup G' is necessarily normal. This can be seen two ways. By the correspondence theorem, all subgroups of G that contain G' correspond to subgroups of G/G', and normality is preserved under this correspondence; since G/G' is abelian, all such subgroups are normal. The other proof is a direct calculation: Let $G' \leq H \leq G$, fix $h \in H$, and consider xhx^{-1}. Since $[x,h] = xhx^{-1}h^{-1} \in H$, also $[x,h]h = xhx^{-1} \in H$. Thus H is fixed under conjugation, and therefore is normal.

Next I claim that $K = \langle x^2 : x \in G\rangle$ contains G'. First note that K comprises all finite products of squares (an inverse of a square is again a square). So I must show that an arbitrary commutator is a product of squares. Indeed, $[x,y] = xyx^{-1}y^{-1} = xyxyy^{-1}x^{-1}x^{-1}y^{-1}x^{-1}x^{-1}xx = (xy)^2(y^{-1}x^{-1}x^{-1})^2(x)^2$.

Wrapping up the solution to the problem: H contains all squares, hence H contains all commutators, hence both H is normal and G/H is abelian.

---

5. Show that every nonzero prime ideal in the ring $\mathbb{Z}[i]$ of Gaussian integers is maximal.

SOLUTION:

The ring of Gaussian integers is a Euclidean domain. Every Euclidean domain is a principal ideal domain. In any principal ideal domain, every nonzero prime ideal is maximal.

---

6. Suppose that R is a noncommutative semisimple ring, and that $|R| = 81$. Describe the center of R as completely as possible.

---

7. Let $f(x) = x^6 + x^4 - 3x^2 - 3$ be a polynomial over $\mathbb{Q}$. Find a splitting field $K \subseteq \mathbb{C}$ for f, and determine the Galois group of f. (Hint: f is not irreducible.)

SOLUTION:

The complete factorization of f over $\mathbb{Q}$ is $f(x) = (x^4-3)(x^2+1)$; after all, none of the roots are in $\mathbb{Q}$, thus there are no linear factors; x^4-3 has no quadratic factor over $\mathbb{Q}$ since $\sqrt{3} \notin \mathbb{Q}$. The roots of f are $\pm\sqrt[4]{3}$, $\pm i\sqrt[4]{3}$, and $\pm i$. Notice that $\mathbb{Q}(\pm\sqrt[4]{3}, \pm i\sqrt[4]{3}, \pm i) = \mathbb{Q}(\sqrt[4]{3}, i\sqrt[4]{3}) = \mathbb{Q}(i, \sqrt[4]{3})$. Thus the splitting field of f is the splitting field of $g(x) = x^4-3$; the polynomials have the same Galois group. We can reach the splitting field $K = \mathbb{Q}(i, \sqrt[4]{3})$ by first adjoining i (a degree 2 extension) to reach $\mathbb{Q}(i)$, and then adjoining $\sqrt[4]{3}$ (a degree 4 extension); note that g remains irreducible over $\mathbb{Q}(i)$, explaining why the second extension had degree 4; thus the splitting field has degree 8 over $\mathbb{Q}$; the Galois group of g has order 8. There exist only five groups of order 8; two of them are non-Abelian. The intermediate field $\mathbb{Q}(\sqrt[4]{3})$ is not normal since it does not contain all the conjugates of $\sqrt[4]{3}$; thus the Galois group has a subgroup that is not normal; thus the Galois group is non-Abelian and is either the Quaternion group Q_8 or the dihedral group $D_{2\times 4}$; but every subgroup of Q_8 is normal and thus the Galois group of g (and of f) must be the dihedral group $D_{2\times 4}$.

---

8. Let $f(x) \in \mathbb{Q}[x]$; let $g(x) = f(x^2)$; let $K \subseteq \mathbb{C}$ be a splitting field for g; let $[K : \mathbb{Q}]$ be odd. Show that f and g have the same Galois group.

---

9. Let $A = \langle\, a, b : 45a = 0,\ 63b = 0,\ 105(a+b) = 0\,\rangle$. Describe A as a direct sum of cyclic groups and determine $|A|$.

10. For each statement, prove it or provide a counterexample.

(a) If R is a principal ideal domain and M is a finitely generated torsion free R-module, then M is free.

(b) If R is an integral domain and M is a finitely generated torsion free R-module, then M is free.

SOLUTION:

(a) A direct proof (without the fundamental structure theorem) is lengthy and I cannot reproduce it. Using the fundamental structure theorem, I know that the module has the structure

$$M \cong R/I_1 \oplus R/I_2 \oplus \cdots \oplus R/I_n,$$

where $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n$. Since M is torsion-free, each ideal I_k is the zero ideal and thus $M \cong R^n$ is free.

(b) Let $R = \mathbb{Z}[x]$. The ideal $M = (2, x)$ is a module over R. The module M is finitely generated and torsion-free. However, M is not free. Since the ideal is not principal, no single element generates it. Any two or more elements are linearly dependent since, for example, $a \cdot b - b \cdot a = 0$. Thus this module cannot have a basis.

PROBLEMS FROM EXAM GIVEN AT UNIVERSITY OF ARIZONA IN JANUARY 1994 (GROVE AND ULMER)

1. Find all real c such that the system

$$\begin{aligned} 2x + c(c-1)y + 3z &= c+1 \\ -2x + c(c-1)y - 3z &= c-1 \end{aligned}$$

has a solution. For such c, find the dimension of the space of solutions.

2. Find the characteristic polynomial, minimal polynomial, rational canonical form, and Jordan canonical form, of the matrix

$$A = \begin{bmatrix} 0 & 4 & 0 \\ 2 & 0 & 8 \\ 0 & -1 & 0 \end{bmatrix}.$$

3. Suppose S is a set and the symmetric group S_4 acts transitively on S. Determine all possibilities for $|S|$.

4. Let $p \in \mathbb{Z}$ be prime. Determine all groups of order $2p$.

SOLUTION:

If $p = 2$ then the order is 4; there are precisely two groups of order 4, namely the cyclic group $\mathbb{Z}_4$ and the Klein group $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. Let $p > 2$. The number of Sylow p-subgroups is congruent to 1 (modulo p) and divides 2; thus there is one Sylow p-subgroup and thus it is normal. The number of Sylow 2-subgroups is odd and divides p; thus there is either one Sylow 2-subgroup or there are p distinct Sylow 2-subgroups. In the former case, the group is $\mathbb{Z}_2 \oplus \mathbb{Z}_p \cong \mathbb{Z}_{2p}$. In the latter case, the p elements of order 2 are pairwise conjugate; I claim that the group must be the dihedral group $D_{2\times p}$. **[How do I establish this claim?]** Fix a nontrivial element a in the normal subgroup of order p; fix a nontrivial element b in one of the subgroups of order 2. Then $a^p = b^2 = 1$; but I need $abab =$ or $baba = 1$.

5. Suppose R is an integral domain (with 1) having only finitely many ideals. Prove that R is a field. If R is only a commutative ring with identity, but not necessarily a domain, is R a field?

SOLUTION:

Consider a nonzero element $x \in R$. Then $(x) \supseteq (x^2) \supseteq \cdots$ is a decreasing chain of ideals; since the number of ideals is finite, the containment in the chain cannot be proper forever; there must be a positive integer n such that $(x^k) = (x^n)$ for $k > n$. Then $x^k \mid x^n$ and $x^n \mid x^k$; thus $x^k = ux^n$ where u is a unit. Then $x^n(x^{k-n} - u) = 0$, and since $x^n \neq 0$ (we are in an integral domain and recall that x was chosen to be nonzero), x^{k-n} is a unit. Thus there is a $y \in R$ such that $x^{k-n}y = 1$; now one sees that x is a unit since $x \cdot x^{k-n-1}y = 1$. Since all nonzero elements are units, R is a field.

If R is only a commutative ring with identity that has finitely many ideals, then R is not necessarily a field. Here is an example. The ring $\mathbb{Z}/4\mathbb{Z}$ is a commutative ring with identity and is finite (and thus has finitely many subsets and at most that many ideals); but $\mathbb{Z}/4\mathbb{Z}$ is not a field.

6. Describe all semisimple rings having 10000 elements.

7. Suppose F, K, and L are fields, with $F \subseteq K \subseteq L$ and $[L : F] < \infty$. For each assertion below, either prove the assertion or provide an example showing the assertion to be false.

(a) If L is Galois over F, then L is Galois over K.
(b) If L is Galois over F, then K is Galois over F.
(c) If L is Galois over K, and K is Galois over F, then L is Galois over F.

8. Suppose F, K are fields with $F \subseteq K$, and suppose $a \in K$ is algebraic over F with $[F(a) : F]$ odd. Show that $F(a^2) = F(a)$.

9. Let M be the $\mathbb{Z}$-module $\mathbb{Z} \oplus (\mathbb{Z}/3\mathbb{Z})$. Give a precise and explicit description of the ring $\mathrm{END}_{\mathbb{Z}}(M)$.

10. Suppose A and B are finite abelian groups each having cyclic Sylow subgroups. View A and B as $\mathbb{Z}$-modules. Calculate $A \otimes_{\mathbb{Z}} B$ and determine its Sylow subgroups.

PROBLEMS FROM EXAM GIVEN AT UNIVERSITY OF ARIZONA IN AUGUST 1993 (GROVE AND ULMER)

1. Determine all matrices A over $\mathbb{Q}$ that have distinct eigenvalues and satisfy $A^2 = 3A - 2I$.

SOLUTION:

Since the matrix satisfies the polynomial $x^2 - 3x + 2 = (x-2)(x-1)$, the minimal polynomial of A is one of $x - 1$, $x - 2$, or $(x-2)(x-1)$. Since the eigenvalues are distinct, the characteristic polynomial of A must have linear factors, yet the characteristic polynomial never has factors that do not appear (possibly with lower multiplicity) in the minimal polynomial. Thus, in this problem, the characteristic polynomial must equal the minimal polynomial. If the minimal and characteristic polynomial is $x - 1$, then A is a 1×1 matrix with eigenvalue 1; thus $A = [1]$. If the minimal and characteristic polynomial is $x - 2$, then A is a 1×1 matrix with eigenvalue 2; thus $A = [2]$. If the minimal and characteristic polynomial is $(x-2)(x-1)$, then A is a 2×2 matrix with eigenvalues 1 and 2; thus it is any 2×2 rational matrix that is similar to the matrix

$$B = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}.$$

Thus A is any of the matrices $P^{-1}BP$, where P ranges over all 2×2 rational invertible matrices.

---

2. Find an orthogonal matrix P that diagonalizes

$$A = \begin{bmatrix} 6 & -2 \\ -2 & 3 \end{bmatrix}.$$

---

3. Let $\alpha = \sqrt{3 + 2\sqrt{3}} \in \mathbb{R}$, and let $F = \mathbb{Q}(\alpha)$.

(a) Find the minimal polynomial for α over $\mathbb{Q}$.

(b) Find explicitly the Galois closure $K \subseteq \mathbb{C}$ of F over $\mathbb{Q}$; that is, find the smallest extension field of F that is Galois over $\mathbb{Q}$.

(c) Determine the Galois group of K over $\mathbb{Q}$.

---

4. Determine the Galois group of a splitting field for $f(x) = x^3 - 2$ over each of the following fields: the field $\mathbb{Q}$ of rational numbers, the field $\mathbb{F}_7$ of seven elements, and the field $\mathbb{F}_9$ of nine elements.

---

5. Show that a finite group G generated by two elements of order 2 is dihedral.

SOLUTION:

Let the two generators be a and b. The element ab must have finite order since the order of the group is finite. Let the order of ab be m. Notice that $(ab)a(ab)a = 1$; thus the two elements a and $c = ab$ satisfy the defining relations $c^m = a^2 = caca = 1$ of the dihedral group of order $2m$; since G may satisfy additional relations, I can conclude only that G is a quotient of the dihedral group; to show that G is the entire dihedral group, I shall now show that G has order $2m$. Since the order of G must divide $2m$, it is sufficient to exhibit $m+1$ distinct elements of G. The m elements ab, $(ab)^2$, $\ldots$, $(ab)^m = 1$ are certainly distinct; I claim that the element a does not appear in this list, thereby exhibiting another element. Assume on the contrary that $a = (ab)^k$; multiplying on the left by a gives $1 = baba \cdots abab$; multiplying on both sides by b gives $1 = aba \cdots aba$; multiplying on both sides by a reduces this further; eventually either $1 = a$ or $1 = b$; either way, a contradiction. In summary, the group G, a quotient of the dihedral group $D_{2\times m}$ of order $2m$, has at least $m+1$ elements; thus $G = D_{2\times m}$.

---

6. Describe all abelian groups of order 63. Prove or disprove that all groups of order 63 are abelian.

SOLUTION:

Since $63 = 3^2 \cdot 7$, any abelian group of order 63 is either $\mathbb{Z}_{63}$ or $\mathbb{Z}_{21} \oplus \mathbb{Z}_3$.

Let G be any group of order 63. The number of Sylow 7-subgroups is congruent to 1 (modulo 7) and divides 9; thus there is one subgroup of order 7 and this subgroup is normal. The number of Sylow 3-subgroups is congruent to 1 (modulo 3) and divides 7; thus there is either one subgroup of order 9, which is normal, or else there are seven subgroups of order 9, which are pairwise conjugate (and thus not normal). The group G is not abelian in the latter case since all subgroups of abelian groups are normal; let me quickly argue that G is always abelian in the former case. A subgroup of order 9, being the square of a prime, is always abelian. The subgroups of order 9 and order 7 are disjoint yet their orders multiply to the full order of the group. Thus G is the direct sum of these two abelian subgroups, and thus G is abelian. One now sees that he only possibility for a nonabelian group is afforded by the latter case; thus nonabelian groups of order 63 exist if and only if the latter case actually occurs; I shall now explore that case further. Let K be the normal subgroup of order 7. Fix H to be one of the seven conjugate subgroups of order 9. **[It seems such a group should exist. Maybe $\langle a, b : a^7 = b^9 = 1, aba^{-1} = b^2 \rangle$.]**

---

7. Let $R = \mathbb{C}[x, y]$.

(a) Find a maximal ideal in R that does not contain xy.

(b) Find a prime ideal in R that is not maximal and does not contain xy.

SOLUTION:

(a) The ideal $(x-1, y-1)$ is maximal and does not contain xy.

(b) Certainly the zero ideal is a prime ideal that is not maximal and does not contain xy. I shall try to find another one. If R were a principal ideal domain, then all nonzero ideals would be maximal and the zero ideal would be the only prime ideal that is not maximal; however, R is not a principal ideal domain and thus there is a possibility of finding prime ideals that are not maximal. The ideals (x), (y), (x^2, xy, y^2) are each prime ideals that are not maximal; however, each contains xy. Since any prime element generates a prime ideal, I need only find a suitable prime element. In general, every prime element is irreducible; in a unique factorization domain, every irreducible element is prime; I am happy to say that R is a unique factorization domain; after all, $\mathbb{C}[x]$ is a PID and thus a UFD, and thus $\mathbb{C}[x][y] = \mathbb{C}[x, y]$ is a UFD since adjoining variables to a UFD gives back a UFD. Therefore, any irreducible element generates a prime ideal. Thus, for example, $(x+1)$ is a prime ideal that is not maximal and does not contain xy.

---

8. Let A be a finitely generated $\mathbb{Z}$-module. Describe $\mathbb{R} \otimes_{\mathbb{Z}} A$ as completely as possible.

SOLUTION:

Since $\mathbb{Z}$ is a principal ideal domain, the structure theorem for finitely generated modules over a principal ideal domain tells me that A is of the form

$$A \cong \mathbb{Z}^k \oplus \mathbb{Z}/I_1 \oplus \mathbb{Z}/I_2 \oplus \cdots \oplus \mathbb{Z}/I_n,$$

where $(0) \subset I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n$. Since tensors distribute over direct sums,

$$\mathbb{R} \otimes_{\mathbb{Z}} A \cong \mathbb{R} \otimes_{\mathbb{Z}} \mathbb{Z}^k \oplus \mathbb{R} \otimes_{\mathbb{Z}} \mathbb{Z}/I_1 \oplus \cdots \oplus \mathbb{R} \otimes_{\mathbb{Z}} \mathbb{Z}/I_n.$$

Now $\mathbb{Z}^k = \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$, and $\mathbb{R} \otimes_{\mathbb{Z}} \mathbb{Z} \cong \mathbb{R}$; thus distributing again gives $\mathbb{R} \otimes_{\mathbb{Z}} \mathbb{Z}^k \cong \mathbb{R}^k$. Furthermore, pick any nonzero $a \in I_1$ (if you wish, pick the generator, but I don't care); then for any $r \otimes (z + I_1)$ in $\mathbb{R} \otimes_{\mathbb{Z}} \mathbb{Z}/I_1$, one has

$$r \otimes (z + I_1) = a(r/a) \otimes (z + I_1) = (r/a) \otimes (az + I_1) = (r/a) \otimes (I_1) = (r/a) \otimes 0 = 0.$$

Thus $\mathbb{R} \otimes_{\mathbb{Z}} \mathbb{Z}/I_1 = 0$, and similarly for the rest. Therefore my most complete description of $\mathbb{R} \otimes_{\mathbb{Z}} A$ is that

$$\mathbb{R} \otimes_{\mathbb{Z}} A \cong \mathbb{R}^k.$$

---

9. Do the following.

(a) Show that if R is a commutative ring, then the set of nilpotent elements of R is an ideal in R.

(b) Prove or disprove that if R is an arbitrary ring, then the set of nilpotent elements of R is an ideal in R.

SOLUTION:

(a) I wish to show that the nilradical $\sqrt{0} = \{\, x \in R \mid x^n = 0 \text{ for some } n \,\}$ is an ideal. Since $0 \in \sqrt{0}$, the nilradical is nonempty. If $a^n = b^m = 0$, then $(a-b)^{n+m-1} = 0$ since each term in the binomial expansion is of the form $ca^k b^{n+m-k-1}$, and if $a^k \neq 0$ then $k < n$ and thus $n + m - k - 1 \geq m$, making $b^{n+m-k-1} = 0$. Thus $\sqrt{0}$ is an additive subgroup of the ring. Finally, if $a^n = 0$, then $(ra)^n = r^n a^n = 0$, and thus $\sqrt{0}$ has the multiplicative absorbtion property. Therefore, $\sqrt{0}$ is an ideal.

(b) Commutativity of the ring was used in the invokation of the binomial expansion. (Although the multiplicative absorbtion was verified only for left multiplication, it clearly works for right multiplication as well.) The binomial theorem does not necessarily hold in an arbitrary ring. Since the portion of the argument using the binomial theorem was the one verifying that $\sqrt{0}$ forms an additive subgroup in a commutative ring, one should be able to find an example of an arbitrary ring in which the nilpotent elements not only do not form an ideal but do not even form an additive subgroup. Here is an example. Consider the ring of 2×2 matrices over, say, the field of real numbers. Then the matrices

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$$

are each nilpotent yet their sum is a matrix that is not nilpotent.

---

10. Show that an integral domain (with 1) that satisfies the descending chain condition for ideals must be a field.

SOLUTION:

Let x be any nonzero element. Then $(x) \supseteq (x^2) \supseteq (x^3) \cdots$ is a descending chain of ideals. The descending chain condition says that there is a positive integer n such that $(x^n) = (x^{n+1})$; thus x^n and x^{n+1} are associate; that is, $ux^n = x^{n+1}$ for some unit u. Cancellation (valid in an integral domain) gives $u = x$. Thus every nonzero element is a unit, and thus the domain is a field.

PROBLEMS FROM EXAM GIVEN AT UNIVERSITY OF ARIZONA IN SPRING 1993

1. Compute the 10th power of the matrix

$$A = \begin{bmatrix} -2 & 2 \\ -6 & 5 \end{bmatrix}.$$

SOLUTION:

Although one approach is to diagonalize the matrix (assuming that this can be done), then raise the diagonal form to the 10th power, and finally "undiagonalize" the result, the following is much simpler. I compute

$$A^2 = \begin{bmatrix} -8 & 6 \\ -18 & 13 \end{bmatrix} \qquad A^4 = \begin{bmatrix} -44 & 30 \\ -90 & 61 \end{bmatrix} \qquad A^8 = \begin{bmatrix} -764 & 510 \\ -1530 & 1021 \end{bmatrix},$$

and then obtain

$$A^{10} = A^2 A^8 = \begin{bmatrix} -8 & 6 \\ -18 & 13 \end{bmatrix} \begin{bmatrix} -764 & 510 \\ -1530 & 1021 \end{bmatrix} = \begin{bmatrix} -3068 & 2046 \\ -6138 & 4093 \end{bmatrix}.$$

2. Compute the Jordan form over $\mathbb{C}$ of the matrix

$$A = \begin{bmatrix} 3 & -1 & 0 \\ 1 & 1 & 0 \\ -6 & -2 & -2 \end{bmatrix}.$$

SOLUTION:

The characteristic polynomial of A is $(x-2)^2(x+2)$. Thus the minimal polynomial either is $(x-2)(x+2)$ or is equal to the characteristic polynomial. Since $(x-2)(x+2)$ does not kill the matrix, the minimal polynomial is equal to the characteristic polynomial. The Jordan form of A is

$$\begin{bmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -2 \end{bmatrix}.$$

3. Let H be the subgroup of S_7, the symmetric group of 7 letters, generated by all 3-cycles. Is the permutation (1234) in H?

SOLUTION:

The 3-cycles generate the alternating subgroup of S_n for $n \geq 3$. Thus H is the alternating group A_7 and does not contain the odd permutation (1234).

4. Give an example of or prove that there does not exist a group of order 5! acting transitively on a set with 9 elements.

SOLUTION:

There does not exist such an action. In any group action, the size of an orbit always equals the index of the stabilizer of a point in that orbit. A transitive action has a single orbit. Thus we must have a stabilizer of index 9; but this is impossible since 9 does not divide 5!.

5. Compute the Galois group of the splitting field of the polynomial

$$f(x) = x^4 + x^2 - 12$$

over each of the following fields: the field $\mathbb{Q}$ of rational numbers, and the field $\mathbb{F}_5$ of five elements.

SOLUTION:

Note that $f(x) = (x^2-3)(x^2+4)$ over $\mathbb{Q}$. Either factor is irreducible over $\mathbb{Q}$. The roots of f are $\pm\sqrt{3}, \pm 2i$. The splitting field of f is the field $\mathbb{Q}(i, \sqrt{3})$. Since $\sqrt{3} \notin \mathbb{Q}(i)$, the splitting field is a degree 4 extension over $\mathbb{Q}$ and thus the Galois group is either the cyclic group $\mathbb{Z}_4$ or the Klein group $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. Since the splitting field contains $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(i)$ as proper intermediate fields, the Galois group must have two proper nontrivial subgroups. The Galois group is $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Note that $f(x) = (x^2-3)(x-1)(x+1)$ over $\mathbb{F}_5$. The factor x^2-3 is irreducible since 3 is not a quadratic residue of 5. Thus the splitting field of f is a degree 2 extension over $\mathbb{F}_5$, and thus the Galois group has order 2. There is only one group of order 2, and thus the Galois group is the cyclic group $\mathbb{Z}_2$.

6. Suppose that $F \subseteq K$ are fields with $\textsc{GaloisGroup}(K/F) \cong D_{2\times 4}$, where $D_{2\times 4}$ is the dihedral group of order 8. How many fields L are there with $F \subseteq L \subseteq K$, and what are their degrees over F?

SOLUTION:

The dihedral group of order 8 contains 10 subgroups; there is one normal subgroup of index 1 (namely the entire group), there is three normal subgroups of index 2 (one generated by the 90° rotation, the other two generated by pairs of perpendicular reflections), there is one normal subgroup of index 2 (generated by the 180° rotation), there are four other subgroups of index 2 (generated by the four reflections), and there is one normal subgroup of index 1 (namely the trivial subgroup).

Thus there are 10 intermediate fields L satisfying $F \subseteq L \subseteq K$. There is one of degree 1 (namely F), three of degree 2, five of degree 4, and one of degree 8 (namely K).

7. Wedderburn's Theorem says that every finite division ring is commutative. Assuming this, is every finite ring without zero divisors commutative? Is every finite ring commutative?

SOLUTION:

I claim that every finite ring without zero divisors is commutative. To prove this using Wedderburn's Theorem, I must show that every finite ring without zero divisors is a division ring; that is, I must show that there is a (unique, simultaneously left and right) identity element, and that every nonzero element has a (unique, simultaneously left and right) inverse. Because the latter argument is shorter, assume for now that there is an identity element, denoted 1. Let $x \neq 0$, and consider the elements x, x^2, x^3, ... Since the ring is finite and contains no zero divisors, none of these elements is zero and the list is finite. Thus $x^n = x^k$ for some $n \geq k$; then $x^n - x^k = x^k(x^{n-k}-1) = 0$; but $x^k \neq 0$ and thus $x^{n-k} = 1$. Then x^{n-k-1} is a (left and right) inverse of x. If y is some other candidate for such an inverse, i.e., $xy = 1$, then multiplying through by x^{n-k-1} on the left gives $y = x^{n-k-1}$, so that y is the same inverse we already found. It remains to show that the ring has an identity element in the first place. Let $x_1, \ldots, x_n$ denote the nonzero elements of the ring. Consider the list $x_1x_1, x_1x_2, x_1x_3, \ldots, x_1x_n$; if $x_1x_j = x_1x_k$, then $x_1(x_j - x_k) = 0$, thus $x_j = x_k$. Similarly with x_1 replaced by the other nonzero elements. Hence each element gives rise, via multiplication, to a permutation of the nonzero elements. In particular, $x_1x_i = x_1$ for some fixed x_i. I claim that x_i is the sought multiplicative identity. Indeed, say $x_ix_j = x_k$, then multiplying by x_1 gives $x_1x_j = x_1x_k$, so that $x_1(x_j - x_k) = 0$, showing $x_j = x_k$. Hence x_i is a left identity. The argument just given was that starting with the knowledge that x_i is a right identity for a particular element, it is necessarily a left identity for all elements. Hence a second application of the argument with left and right reversed shows that x_i is also a right identity for all elements. Finally, if y were another candidate for identity, then $x_i = x_iy = y$, showing the identity to be unique.

I shall show by example that not every finite ring is commutative. Consider the ring of all 2×2 matrices over $\mathbb{F}_2$, the field of two elements. This ring is finite (there are precisely sixteen matrices) but is not commutative; for example,

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}.$$

Note that this ring contains zero divisors; for example, take either matrix used in the example above and square it; you will obtain the zero matrix.

8. Let R be a commutative ring, and let $\mathfrak{m} \subseteq R$ be an ideal. Prove that R is a local ring with maximal ideal $\mathfrak{m}$ if and only if every element of R not in $\mathfrak{m}$ is invertible.

SOLUTION:

Let R be local. Then, by definition, R has a unique maximal ideal, and thus $\mathfrak{m}$ is that ideal. Let $x \in R$ be an element that is not in $\mathfrak{m}$. I wish to show that x is invertible. I will do this by showing that if x were not invertible, then x would be in $\mathfrak{m}$; after all, if x were not invertible, then (x) would be a proper ideal contained in some maximal ideal, and thus x would lie in the unique maximal ideal $\mathfrak{m}$.

Let R be such that $\mathfrak{m}$ is a maximal ideal such that every element outside $\mathfrak{m}$ is invertible. I wish to show that $\mathfrak{m}$ is the unique maximal ideal, thus showing that R is local. I claim that $\mathfrak{m}$ consists of all nonunits. Since all maximal ideals are proper, $\mathfrak{m}$ contains no units. Furthermore, any nonunit must lie in $\mathfrak{m}$ since all elements outside $\mathfrak{m}$ are invertible. Thus $\mathfrak{m}$ consists of all nonunits. Finally, I claim that any proper ideal is contained in $\mathfrak{m}$. After all, any proper ideal consists entirely of nonunits, and thus is contained in $\mathfrak{m}$. It follows that any maximal ideal, being contained in $\mathfrak{m}$, must equal $\mathfrak{m}$. Thus $\mathfrak{m}$ is the unique maximal ideal.

---

9. Let R be the polynomial ring $\mathbb{C}[x, y]$. For each of the following ideals, state whether the ideal is maximal, whether the ideal is prime, and whether the ideal is radical.
(a) (xy^2)
(b) $(x - y^2)$
(c) $(x - \pi, \pi y - 1)$
(d) $(y - x^2, y - 1)$
(e) (0)

---

10. Let M be the group $\mathbb{Z}/25\mathbb{Z} \times \mathbb{Z}/35\mathbb{Z}$, viewed as a $\mathbb{Z}$-module. Let R_1 be the ring $\mathbb{Z}[1/7]$ and let R_2 be the ring $\mathbb{Z}S^{-1}$ where S is the multiplicatively closed subset $\mathbb{Z} - 7\mathbb{Z} \subseteq \mathbb{Z}$. Give the structure of the modules $R_1 \otimes_{\mathbb{Z}} M$ and $R_2 \otimes_{\mathbb{Z}} M$.

PROBLEMS FROM EXAM GIVEN AT UNIVERSITY OF ARIZONA IN FALL 1992

1. For what values of c is the following system solvable?

$$\begin{aligned} u + v + 2w &= 0 \\ 2u + 3v - w &= 5 \\ 3u + 4v + w &= c \end{aligned}$$

---

2. Find a real matrix, satisfying $A^7 = I$, that is not diagonalizable over the reals.

SOLUTION:

---

3. Show that a group of order 48 must have a normal subgroup whose order is a power of 2.

SOLUTION:

Note $48 = 2^4 \cdot 3$. The Sylow 2-subgroups of the group have order 16 and the number of them is odd and divides 3; thus there is either one, or else there are three. If there is only one, then it is normal, and I am done. Now consider the case that there are three subgroups of order 16; call them H_1, H_2, and H_3. Note that they are pairwise conjugate. Consider the subgroup $H = H_1 \cap H_2 \cap H_3$. **[Now what?]**

4. Let k be a finite field with 7 elements. Let $f(x) = x^3 - 3$ and let α be a root of f. Finally, let $l = k(\alpha)$. Factor f into irreducible polynomials over l.

SOLUTION:

Adjoining one root of f will bring in the other roots if and only if the ground field k contains all cube roots of unity. In fact, the cube roots of unity are 1, 2, and 4. Thus, over l, there is the factorization

$$f(x) = (x - \alpha)(x - 2\alpha)(x - 4\alpha).$$

5. Write down a prime ideal in $\mathbb{C}[x, y]$ that is not maximal. Write down an ideal in $\mathbb{C}[x, y]$ that is not principal.

SOLUTION:

The ideal (x) is prime but not maximal. The ideal (x, y) is not principal.

6. Let G be the group of real 2×2 matrices that have determinant 1, and let H be the subgroup of diagonal matrices.

(a) Find the normalizer of H in G, denoted $N_G(H)$.
(b) Find representatives for the cosets in $N_G(H)/H$.

7. Give an example of two non-trivial modules M, N over a ring R such that $M \otimes_R N = 0$.

SOLUTION:

View the abelian groups $\mathbb{Q}$ and $\mathbb{Z}/4\mathbb{Z}$ as $\mathbb{Z}$-modules. I claim that $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/4\mathbb{Z} = 0$. Given any $(a/b) \otimes (k + 4\mathbb{Z})$, factor out a 4 from the left and move it to the right to obtain 0 as follows:

$$(a/b) \otimes (k + 4\mathbb{Z}) = (4a/4b) \otimes (k + 4\mathbb{Z}) = (a/4b) \otimes (4k + 4\mathbb{Z}) = (a/4b) \otimes (0 + 4\mathbb{Z}) = 0.$$

8. Let $0 \to A \to B \to C \to 0$ be an exact sequence of abelian groups. Prove that if B has torsion elements, then either A or C must also have torsion elements.

SOLUTION:

View A, B, C as $\mathbb{Z}$-modules, identify A with its image in B, and identify C with B/A. This gives me the following reformulation of the problem. I wish to show that if N is a submodule of the module M, where M has torsion, then either N or M/N has torsion. I will require M to be over an integral domain, but not necessarily over a principal ideal domain. If N contains torsion elements of M, then N itself has torsion, and I am done. Now assume that N contains no torsion elements of M; I claim that M/N has torsion. Let $x \in M$ be a torsion element, so that $rx = 0$ for some $r \neq 0$ from the integral domain; then the coset $x + N$ (which is nonzero) has torsion since $r(x + N) = rx + N = 0$.

Note that I required the module to be defined over an integral domain merely because most authors only define the torsion concept over an integral domain, and, furthermore, the theorems concerning torsion assume that one is over an integral domain (and sometimes even over a principal ideal domain). However, I did not use any theorems, and the argument above should be valid over any (even noncommutative) ring with identity, as long as we have a suitable definition for an element to be torsion (and why not take either the definition that an element is torsion if its annihilator is nonzero, or perhaps the stronger requirement that the annihilator contain a ring element that is not a zero divisor).

9. Suppose that T is a linear transformation on $\mathbb{C}^n$ with $T^3 = I$. Show that T must be diagonalizable.

SOLUTION:

To ask whether T as a linear transformation is diagonalizable is to ask whether there exists a basis of $\mathbb{C}^n$ such that the matrix representation of T (with respect to this basis) is diagonal. The equivalent question is whether the matrix of T (with respect to any basis, say the canonical one) is similar to a diagonal matrix. The matrix of T satisfies the polynomial $x^3 - 1 = (x - 1)(x - e^{2\pi i/3})(x - e^{4\pi i/3})$; thus the minimal polynomial of T divides this polynomial, and thus the minimal polynomial of T has distinct linear factors. Invoking the theorem that a matrix is diagonalizable if and only if its minimal polynomial has distinct linear factors gives that the matrix of T is diagonalizable, and thus T is diagonalizable.