Algebra - Spring 2011

Daren Cheng
Jesse Madnick

Last updated: September 2013

Acknowledgments & Disclaimers

Some of the solutions contained herein are my own, but many are not. I am indebted to Daren Cheng for sharing with me his solutions to several full-length exams. I'd also like to acknowledge Zev Chonoles, Fernando Shao, and my algebra professors Dan Bump and Akshay Venkatesh, all of whom patiently tolerated my many questions.

I am not exactly an algebraist. My writing style tends towards the wordy side, and my preferred proofs are rarely the most elegant ones. Still, I hope to keep these solutions free of any substantial errors. For this reason: if you notice any errors (typographical or logical), *please* let me know so I can fix it! Your speaking up would be a kindness for future students who may be struggling to make sense of an incorrect expression. I can be reached at jmadnick@math.stanford.edu.

1. (a) Prove that if G is a finite group and H is a proper subgroup, then G is not a union of conjugates of H. (Hint: the conjugates all contain the identity.)

Solution: Let $H < G$ be a proper subgroup. Note that the number of conjugates of H is $|G\colon N_G(H)|$. Note also that each conjugate contains $|H|$ elements, and that each conjugate contains the identity. Therefore, each conjugate can contain at most $|H| - 1$ elements that belong to no other conjugate. Thus,

$$\begin{aligned}\left|\bigcup_{g \in G} gHg^{-1}\right| &\leq \frac{|G|}{|N_G(H)|}(|H| - 1) + 1 \\ &\leq \frac{|G|}{|H|}(|H| - 1) + 1 \\ &= |G| - \frac{|G|}{|H|} + 1 \\ &< |G|\end{aligned}$$

We conclude that the union of conjugates of H is a proper subset of G.

(b) Suppose G is a (finite) transitive group of permutations of a finite set X of n objects, $n > 1$. Prove that there exists $g \in G$ with no fixed points of X. (Hint: use part (a).)

Solution: Let $x \in X$ be arbitrary. If $\operatorname{Stab}(x) = G$, then every $g \in G$ fixes x, so we're done.

Otherwise, $\operatorname{Stab}(x) < G$ is a proper subgroup. Since G acts transitively on X, we can write $X = \{g_1 x, \ldots, g_n x\}$ for some $g_1, \ldots, g_n \in G$. By part (a), we have

$$\bigcup_{i=1}^{n} g_i \operatorname{Stab}(x)\, g_i^{-1} \subsetneq G.$$

Since $g_i \operatorname{Stab}(x)\, g_i^{-1} = \operatorname{Stab}(g_i x)$, we have

$$\bigcup_{i=1}^{n} \operatorname{Stab}(g_i x) \subsetneq G.$$

Thus, there exists $g \in G$ such that $g \notin \operatorname{Stab}(g_i x)$ for any $i = 1, \ldots, n$. That is, $g \notin \operatorname{Stab}(y)$ for any $y \in X$, so g has no fixed points.

2. (a) Let ζ denote a complex primitive 25th root of unity. Show that $x^5 - 5$ has no roots in $\mathbb{Q}[\zeta]$.

> *Solution:* Note that $\mathbb{Q}(\zeta)/\mathbb{Q}$ is Galois, with Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/25\mathbb{Z})^\times \cong \mathbb{Z}/20\mathbb{Z}$. Since $\mathbb{Z}/20\mathbb{Z}$ has only one subgroup of order 4, it follows that $\mathbb{Q}(\zeta)$ has only one subfield of degree 5 over $\mathbb{Q}$.
>
> Suppose, then, for the sake of contradiction, that $x^5 - 5$ has a root in $\mathbb{Q}(\zeta)$. Since $\mathbb{Q}(\zeta)/\mathbb{Q}$ is normal and $x^5 - 5 \in \mathbb{Q}[x]$ is irreducible (by Eisenstein's criterion), it follows that $x^5 - 5$ has all of its roots in $\mathbb{Q}(\zeta)$. In particular, both $\sqrt[5]{5}, \sqrt[5]{5}\,\omega_5 \in \mathbb{Q}(\zeta)$, where ω_5 is a primitive 5th root of unity. Thus, $\mathbb{Q}(\sqrt[5]{5})$ and $\mathbb{Q}(\sqrt[5]{5}\,\omega_5)$ are (distinct) subfields of $\mathbb{Q}(\zeta)$ of degree 5 over $\mathbb{Q}$, which contradicts the preceding paragraph.

(b) If $\alpha^5 = 5$, show that α is not a 5th power in $\mathbb{Q}[\zeta, \alpha]$.

> *Solution:* Let $F = \mathbb{Q}(\zeta)$. Let $m_{\alpha/F} \in F[x]$ denote the minimal polynomial of α. We claim that $\deg(m_{\alpha/F}) = [F(\alpha) \colon F] = 5$.
>
> To see this, note that $F(\alpha)/F$ is Galois (by virtue of being the splitting field of $x^5 - 5 \in F[x]$). For any $\sigma \in \mathrm{Gal}(F(\alpha)/F)$, we have $\sigma(\sqrt[5]{5}) = \sqrt[5]{5}\,\omega_5^k$ for some $k \in \{0, \ldots, 4\}$. This gives an injective homomorphism
>
> $$\mathrm{Gal}(F(\alpha)/F) \longrightarrow \{\text{5th roots of unity}\} \cong \mathbb{Z}/5\mathbb{Z}$$
> $$\sigma \mapsto \frac{\sigma(\sqrt[5]{5})}{\sqrt[5]{5}} = \omega_5^k \mapsto k$$
>
> Thus, $[F(\alpha) \colon F] = |\mathrm{Gal}(F(\alpha)/F)| \mid 5$. Since $\alpha \notin F$ by part (a), we have $[F(\alpha) \colon F] \neq 1$, so that $\deg(m_{\alpha/F}) = [F(\alpha) \colon F] = 5$.
>
> Thus, $m_{\alpha/F}(x) = x^5 - 5$. Therefore, $N_{F(\alpha)/F}(\alpha) = (-1)^5(-5) = 5$.
>
> Suppose for the sake of contradiction that α were a 5th power in $\mathbb{Q}[\zeta, \alpha] = F(\alpha)$, say $\alpha = \beta^5$ for some $\beta \in F(\alpha)$. Let $\gamma = N_{F(\alpha)/F}(\beta) \in F$. Then
>
> $$\gamma^5 = N_{F(\alpha)/F}(\beta)^5 = N_{F(\alpha)/F}(\beta^5) = N_{F(\alpha)/F}(\alpha) = 5.$$
>
> Thus, there exists an element $\gamma \in F$ with $\gamma^5 = 5$, which contradicts part (a).

3. (a) Let $q = p^n$, p prime, and let $\mathbb{F}_q$ denote a finite field of q elements. How many monic irreducible polynomials of degree 2 are there over $\mathbb{F}_q$? How many monic irreducible polynomials of degree 3 are there over $\mathbb{F}_q$? (Hint: Think about elements of $\mathbb{F}_{q^2}$ and $\mathbb{F}_{q^3}$.)

Solution: Note that every monic irreducible quadratic over $\mathbb{F}_q$ is the minimal polynomial of either of its two roots. Conversely, any element of $\mathbb{F}_{q^2} - \mathbb{F}_q$ has as its minimal polynomial a monic irreducible quadratic over $\mathbb{F}_q$. Therefore,

$$\#\text{ of irreducible degree 2 polynomials over } \mathbb{F}_q = \frac{1}{2}(q^2 - q).$$

A completely analogous argument shows that

$$\#\text{ of irreducible degree 3 polynomials over } \mathbb{F}_q = \frac{1}{3}(q^3 - q).$$

Alternate Solution: Let $\psi(n) = \#$ of irreducible polynomials of degree n in $\mathbb{F}_q[x]$. Note that $x^{q^2} - x \in \mathbb{F}_q[x]$ is the product of all irreducible linear and quadratic polynomials in $\mathbb{F}_q[x]$. Counting degrees shows that $q^2 = \psi(1) + 2\psi(2) = q + 2\psi(2)$, so that

$$\psi(2) = \frac{1}{2}(q^2 - q).$$

Similarly, $x^{q^3} - x \in \mathbb{F}_q[x]$ is the product of all irreducible linear and cubic polynomials in $\mathbb{F}_q[x]$. Counting degrees shows that $q^3 = \psi(1) + 3\psi(3) = q + 3\psi(3)$, so that

$$\psi(3) = \frac{1}{3}(q^3 - q).$$

3. (b) Determine the number of conjugacy classes in the group $\mathrm{GL}_3(\mathbb{F}_q)$. (Hint: Use canonical forms of modules over a principal ideal domain. One canonical form would use part (a), but you can also solve part (b) without using part (a).)

Solution via Rational Canonical Form: Note that every conjugacy class in $\mathrm{GL}_3(\mathbb{F}_q)$ is represented by a unique matrix in rational canonical form. Thus, we count the number of rational canonical forms that lie in $\mathrm{GL}_3(\mathbb{F}_q)$. Three types can occur. Namely:

$$A_1 = \begin{pmatrix} 0 & 0 & -b_0 \\ 1 & 0 & -b_1 \\ 0 & 1 & -b_2 \end{pmatrix} \quad A_2 = \begin{pmatrix} 0 & -a_0 b_0 & 0 \\ 1 & -(a_0+b_0) & 0 \\ 0 & 0 & -a_0 \end{pmatrix} \quad A_3 = \begin{pmatrix} -b_0 & 0 & 0 \\ 0 & -b_0 & 0 \\ 0 & 0 & -b_0 \end{pmatrix},$$

corresponding to the $\mathbb{F}_q[x]$-modules

$$V_1 = \frac{\mathbb{F}_q[x]}{(x^3 + b_2 x^2 + b_1 x + b_0)}, \quad V_2 = \frac{\mathbb{F}_q[x]}{(x+a_0)} \oplus \frac{\mathbb{F}_q[x]}{(x+a_0)(x+b_0)},$$

$$V_3 = \frac{\mathbb{F}_q[x]}{(x+b_0)} \oplus \frac{\mathbb{F}_q[x]}{(x+b_0)} \oplus \frac{\mathbb{F}_q[x]}{(x+b_0)}.$$

We now note that

$$\begin{aligned} \det(A_1) = -b_0 &\implies \text{There are } q^2(q-1) \text{ invertible matrices of form } A_1. \\ \det(A_2) = -a_0^2\, b_0 &\implies \text{There are } (q-1)^2 \text{ invertible matrices of form } A_2. \\ \det(A_3) = -b_0^3 &\implies \text{There are } (q-1) \text{ invertible matrices of form } A_3. \end{aligned}$$

Therefore,

$$\begin{aligned} \#\text{ of conjugacy classes in } \mathrm{GL}_3(\mathbb{F}_q) &= q^2(q-1) + (q-1)^2 + (q-1) \\ &= q(q+1)(q-1) \end{aligned}$$

3. (b) Determine the number of conjugacy classes in the group $GL_3(\mathbb{F}_q)$. (Hint: Use canonical forms of modules over a principal ideal domain. One canonical form would use part (a), but you can also solve part (b) without using part (a).)

Solution via Jordan Canonical Form: Note that every conjugacy class in $GL_3(\mathbb{F}_q)$ determines a unique $\mathbb{F}_q[x]$-module structure on the $\mathbb{F}_q$-vector space $V = (\mathbb{F}_q)^3$. Thus, we count the number of $\mathbb{F}_q[x]$-module structures on $(\mathbb{F}_q)^3$ that have invertible Jordan canonical forms. Five main types can occur:

Type	Canonical form type	Number of such invertible forms
1	$\dfrac{\mathbb{F}_q[x]}{(\text{irreducible cubic})}$	$\frac{1}{3}(q^3 - q)$
2	$\dfrac{\mathbb{F}_q[x]}{(x-\lambda)} \oplus \dfrac{\mathbb{F}_q[x]}{(\text{irreducible quadratic})}$	$\frac{1}{2}(q^2 - q)(q-1)$
3	$\dfrac{\mathbb{F}_q[x]}{(x-\lambda)^3}$	$q-1$
4	$\dfrac{\mathbb{F}_q[x]}{(x-\lambda_1)} \oplus \dfrac{\mathbb{F}_q[x]}{(x-\lambda_2)} \oplus \dfrac{\mathbb{F}_q[x]}{(x-\lambda_3)}$	$(q-1) + (q-1)(q-2) + \binom{q-1}{3}$
5	$\dfrac{\mathbb{F}_q[x]}{(x-\lambda_1)} \oplus \dfrac{\mathbb{F}_q[x]}{(x-\lambda_2)^2}$	$(q-1) + (q-1)(q-2)$

The count for Type 1 and Type 2 follows from part (a).

The count for Type 3 is clear.

The count for Type 4 follows by distinguishing three cases:
(i) $\lambda_1 = \lambda_2 = \lambda_3$: There are $q-1$ forms.
(ii) Exactly two λ_i are the same: There are $(q-1)(q-2)$ forms.
(iii) $\lambda_1, \lambda_2, \lambda_3$ all distinct: There are $\frac{1}{6}(q-1)(q-2)(q-3)$ forms.

The count for Type 5 follows by distinguishing two cases:
(i) $\lambda_1 = \lambda_2$: There are $q-1$ forms.
(ii) $\lambda_1 \neq \lambda_2$: There are $(q-1)(q-2)$ forms.

Thus, in total, we have that

$$\begin{aligned}
\#\text{ of conjugacy classes in } GL_3(\mathbb{F}_q) &= \frac{1}{3}(q^3 - q) + \frac{1}{2}(q^2 - q)(q-1) \\
&\quad + \left[(q-1) + (q-1)(q-2) + \binom{q-1}{3}\right] \\
&\quad + (q-1) + [(q-1) + (q-1)(q-2)] \\
&= q(q+1)(q-1).
\end{aligned}$$

4. (a) Let K be an algebraically closed field. Suppose $S \subset K^n$ is the set of common zeros of a family of polynomials $\{f_i\} \subset K[x_1, \ldots, x_n]$, and assume S is non-empty. Suppose

$$r = \frac{g}{d} \in K(x_1, \ldots, x_n)$$

is a rational function such that the polynomial d is non-zero at all points of S. Thus r defines a K-valued function on S. Prove that there is a polynomial $h \in K[x_1, \ldots, x_n]$ so that $h(x) = r(x)$ for all $x \in S$. (Hint: Consider the ideal generated by the f_i and d.)

Notation: For a subset $S \subset K^n$, we let $\mathcal{I}(S) = \{f \in K[x_1, \ldots, x_n] \colon f(p) = 0\ \forall p \in S\}$.

Solution: Consider the ideal (f_i, d). Since d is non-zero at all points of S, we have

$$\mathcal{Z}(\{f_i\}, d) := \{x \in K^n \colon f_i(x) = 0\ \forall i \text{ and } d(x) = 0\} = \emptyset.$$

Thus, by the Nullstellensatz,

$$\operatorname{rad}(\{f_i\}, d) = \mathcal{I}(\mathcal{Z}(\{f_i\}, d)) = \mathcal{I}(\emptyset) = K[x_1, \ldots, x_n],$$

and so $(\{f_i\}, d) = K[x_1, \ldots, x_n]$.

In particular, $g \in (\{f_i\}, d)$, so there exist polynomials $p_1, \ldots, p_\ell, h \in K[x_1, \ldots, x_n]$ such that $g = p_1 f_{i_1} + \ldots + p_\ell f_{i_\ell} + hd$, so that

$$r = \frac{g}{d} = p_1 \frac{f_{i_1}}{d} + \ldots + p_\ell \frac{f_{i_\ell}}{d} + h.$$

Since $f_{i_j}(x) = 0$ and $d(x) \neq 0$ for all $x \in S$, we have $r(x) = h(x)$ for all $x \in S$.

(b) Give a counterexample to part (a) if K is not algebraically closed, by taking $K = \mathbb{Q}$, $n = 2$, $f_1 = x^2 + y^2 - 1$, and $r = 1/(y - x)$, and showing that there is no $h \in \mathbb{Q}[x, y]$ with $h(x, y) = r(x, y)$ on $S = \{(x, y) \in \mathbb{Q}^2 \colon x^2 + y^2 = 1\}$. (Hint: You may use without proof the fact that any polynomial $g \in \mathbb{Q}[x, y]$ that vanishes on S must be a multiple of $x^2 + y^2 - 1$.)

Solution: Suppose for the sake of contradiction that there exists an $h \in \mathbb{Q}[x, y]$ with $h(x, y) = \frac{1}{y-x}$ on S. Then $h(x, y)(y - x) - 1 = 0$ on S, so by the Hint:

$$h(x, y)(y - x) - 1 = p(x, y)(x^2 + y^2 - 1) \text{ on } S \qquad (*)$$

for some $p \in \mathbb{Q}[x, y]$.

Let $q(x) = p(x, x)$. Setting $x = y$ in $(*)$ gives $-1 = q(x)(2x^2 - 1)$, so

$$q(x)(2x^2 - 1) + 1 = 0 \quad \forall x \in \mathbb{Q}.$$

But this is impossible since polynomials of one variable have at most finitely many roots. Contradiction.

5. Find, with proof, all algebraic integers in the field $\mathbb{Q}[\sqrt{6}]$. For which of the integer primes $p = 2, 3, 5, 7, 11$ is there exactly one prime ideal in the ring of integers lying over the prime ideal $(p) \subset \mathbb{Z}$?

Notation: Let $\mathcal{O}_K = \{\text{algebraic integers in } \mathbb{Q}[\sqrt{6}]\}$. Also, for a prime ideal $(p) \subset \mathbb{Z}$, we let $(p)^e = p\mathcal{O}_K$ denote the ideal generated by p in $\mathcal{O}_K$.

Solution: We claim that $\mathcal{O}_K = \mathbb{Z}[\sqrt{6}]$.

One inclusion is simple: since $\sqrt{6}$ is a root of $x^2 - 6 \in \mathbb{Z}[x]$, we have $\sqrt{6} \in \mathcal{O}_K$, so $\mathbb{Z}[\sqrt{6}] \subset \mathcal{O}_K$. It remains to show the reverse inclusion.

Let $\zeta = a + b\sqrt{6} \in \mathcal{O}_K \subset \mathbb{Q}[\sqrt{6}]$. Let $m_\zeta \in \mathbb{Q}[x]$ denote the minimal polynomial of ζ over $\mathbb{Q}$. Note that

$$m_\zeta(x) = (x - (a + b\sqrt{6}))(x - (a - b\sqrt{6})) = x^2 - 2ax + (a^2 - 6b^2).$$

Since $\zeta \in \mathcal{O}_K$, we have $m_\zeta \in \mathbb{Z}[x]$, so that $2a \in \mathbb{Z}$ and $a^2 - 6b^2 \in \mathbb{Z}$. Thus, $6 \cdot (2b)^2 = 4(a^2 - 6b^2) - (2a)^2 \in \mathbb{Z}$. Since 6 is square-free, it follows that $2b \in \mathbb{Z}$.

Write $a = x/2$ and $b = y/2$ for some $x, y \in \mathbb{Z}$. Since $a^2 - 6b^2 \in \mathbb{Z}$, it follows that $x^2 - 6y^2 \equiv 0 \pmod 4$. This implies (after short casework) that x and y must be even, and so $a, b \in \mathbb{Z}$. This proves that $\zeta \in \mathbb{Z}[\sqrt{6}]$.

By definition, a prime $\mathfrak{q} \subset \mathbb{Z}[\sqrt{6}]$ *lies above* the prime $(p) \subset \mathbb{Z}$ iff $\mathfrak{q} \cap \mathbb{Z} = (p)$. One can check that this is equivalent to saying that the prime $\mathfrak{q}$ has $\mathfrak{q} \supset (p)^e$. Moreover, the primes containing $(p)^e$ are in bijection with the prime ideals of $\mathbb{Z}[\sqrt{6}]/(p)^e$. That is:

$$\left\{\text{Primes } \mathfrak{q} \subset \mathbb{Z}[\sqrt{6}] \text{ above } (p)\right\} = \left\{\text{Primes } \mathfrak{q} \subset \mathbb{Z}[\sqrt{6}] \text{ containing } (p)^e\right\}$$
$$\leftrightarrow \left\{\text{Prime ideals of } \frac{\mathbb{Z}[\sqrt{6}]}{(p)^e} \cong \frac{\mathbb{Z}[x]}{(p, x^2 - 6)} \cong \frac{\mathbb{F}_p[x]}{(x^2 - 6)}\right\}$$

We now claim that for $p = 2, 3, 7, 11$, there is only one prime ideal above (p).

$p = 2$: Since $x^2 - 6 = x^2$ in $\mathbb{F}_2[x]$, we have $\frac{\mathbb{Z}[\sqrt{6}]}{(2)^e} \cong \frac{\mathbb{F}_2[x]}{(x^2-6)} = \frac{\mathbb{F}_2[x]}{(x^2)}$, which has only one prime ideal. Thus, there is only one prime $\mathfrak{q} \subset \mathbb{Z}[\sqrt{6}]$ above (2). (Namely, $\mathfrak{q} = (2, \sqrt{6})$.)

$p = 3$: Analogous to the case $p = 2$.

$p = 5$: Since $x^2 - 6 = x^2 - 1 = (x + 1)(x - 1)$ in $\mathbb{F}_5[x]$, we have that

$$\frac{\mathbb{Z}[\sqrt{6}]}{(5)^e} \cong \frac{\mathbb{F}_5[x]}{(x^2 - 6)} \cong \frac{\mathbb{F}_2[x]}{(x + 1)} \times \frac{\mathbb{F}_5[x]}{(x - 1)}$$

is a product of two fields, hence has two prime ideals. Thus, there are two prime ideals $\mathfrak{q}_1, \mathfrak{q}_2$ above (5). (In general, a product of n fields will have n prime ideals.)

$p = 7$: Since $x^2 - 6 = x^2 + 1$ is irreducible in $\mathbb{F}_7[x]$, we have that $\frac{\mathbb{Z}[\sqrt{6}]}{(7)^e} \cong \frac{\mathbb{F}_7[x]}{(x^2-6)} = \frac{\mathbb{F}_2[x]}{(x^2+1)}$ is a field, hence has one prime ideal. Thus, there is only one prime $\mathfrak{q} \subset \mathbb{Z}[\sqrt{6}]$ above (7), namely $\mathfrak{q} = (7)^e$. (In other words: $\frac{\mathbb{Z}[\sqrt{6}]}{(7)^e}$ is a field, so $(7)^e$ is maximal.)

$p = 11$: Analogous to the case $p = 7$.

6. Let V be a nonzero finite-dimensional vector space over an algebraically closed field k, and let $T\colon V \to V$ be a linear endomorphism.

(a) What does the theorem on Jordan canonical form say about T acting on V? Prove it (including the uniqueness aspects) using the structure theorem for finitely generated modules over a PID.

Theorem: There exists a basis for V with respect to which the matrix of T is a block diagonal matrix whose blocks are the Jordan blocks of the elementary divisors of V. Moreover, this form is unique up to permutation of the Jordan blocks.

Proof: Regard V as a $k[x]$-module, where $x \in k[x]$ acts on V as the linear map T. Since $k[x]$ is a PID and V is finitely generated as a $k[x]$-module, the structure theorem implies that

$$V \cong k[x]^r \oplus \frac{k[x]}{(p_1^{\alpha_1})} \oplus \cdots \oplus \frac{k[x]}{(p_t^{\alpha_t})},$$

for some primes $p_i \in k[x]$ (not necessarily distinct) and some $r \geq 0$ and $\alpha_i \geq 1$.

Since $\dim_k(V) < \infty$ whereas $\dim_k(k[x]) = \infty$, we must have $r = 0$. Since k is algebraically closed, every prime p_i is linear: $p_i(x) = x - \lambda_i$ for some $\lambda_i \in k$. Thus,

$$V \cong \frac{k[x]}{(x-\lambda_1)^{\alpha_1}} \oplus \cdots \oplus \frac{k[x]}{(x-\lambda_t)^{\alpha_t}}. \qquad (*)$$

Note that $\{\overline{1}, (\overline{x}-\lambda_i), \ldots, (\overline{x}-\lambda_i)^{\alpha_i - 1}\}$ is a basis for the k-vector space $k[x]/(x-\lambda_i)^{\alpha_i}$. (I omit the proof of this.) With respect to this basis, multiplication by $x \in k[x]$ acts as:

$$x\colon \begin{cases} \overline{1} & \mapsto \lambda_i \overline{1} + (\overline{x} - \lambda_i) \\ (\overline{x} - \lambda_i) & \mapsto \lambda_i(\overline{x} - \lambda_i) + (\overline{x} - \lambda_i)^2 \\ \cdots & \\ (\overline{x} - \lambda_i)^{\alpha_i - 2} & \mapsto \lambda_i(\overline{x} - \lambda_i)^{\alpha_i - 2} + (\overline{x} - \lambda_i)^{\alpha_i - 1} \\ (\overline{x} - \lambda_i)^{\alpha_i - 1} & \mapsto \lambda_i(\overline{x} - \lambda_i)^{\alpha_i} \end{cases}$$

Thus, with respect to this basis of $k[x]/(x-\lambda_i)^{\alpha_i}$, the linear transformation T has the form of an $\alpha_i \times \alpha_i$ Jordan block:

$$\begin{pmatrix} \lambda_i & 1 & & \\ & \lambda_i & 1 & \\ & & \ddots & \ddots \\ & & & \lambda_i \end{pmatrix}$$

Applying this to each of the direct summands $k[x]/(x-\lambda_i)^{\alpha_i}$ of V, we obtain a k-vector space basis of V with respect to which the matrix of T takes the desired form.

By the uniqueness part of the structure theorem for finitely generated modules over a PID, the primes $p_i(x) = x - \lambda_i$ and the powers α_i are uniquely determined by T. Thus, the decomposition $(*)$ is unique up to permutation of direct summands, so that the Jordan form of T is unique up to permutation of the Jordan blocks.

6. Let V be a nonzero finite-dimensional vector space over an algebraically closed field k, and let $T\colon V \to V$ be a linear endomorphism.

(b) Using the Jordan canonical form, prove that T is diagonalizable if and only if its minimal polynomial has no repeated roots.

Solution: Let $m_T(x)$ denote the minimal polynomial of T.

($\Longrightarrow$) Suppose T is diagonalizable. Then there exists a basis of V with respect to which the matrix of T is diagonal. Let D be this diagonal matrix, and let $m_D(x)$ denote its minimal polynomial. Since minimal polynomials are invariant under change of basis, we have $m_T(x) = m_D(x)$. Since the minimal polynomial of diagonal matrix has as its roots the *distinct* elements on the diagonal, it follows $m_D(x)$ has no repeated roots.

($\Longleftarrow$) Suppose that $m_T(x)$ has no repeated roots. Let J denote the Jordan form (matrix) of T, and let $m_J(x)$ denote the minimal polynomial of J. Since minimal polynomials are invariant under change of basis, we have $m_T(x) = m_J(x)$, and so $m_J(x)$ has no repeated roots.

Suppose that J has the block diagonal form

$$J = \begin{pmatrix} J_1 & & \\ & \ddots & \\ & & J_t \end{pmatrix},$$

where each J_i is a Jordan block of size α_i with eigenvalue λ_i.

Note that $m_J(x) = \operatorname{lcm}[m_{J_1}(x), \dots, m_{J_t}(x)]$. Note also that $m_{J_i}(x) = (x - \lambda_i)^{\alpha_i}$. Thus, since $m_J(x)$ has no repeated roots, we must have each $\alpha_i = 1$. In other words, every Jordan block has size 1, so J is a diagonal matrix.

7. Suppose $1 \to N \xrightarrow{i} G \xrightarrow{j} K \to 1$ is an exact sequence of groups, with G finite. Let $P \subset G$ be a p-Sylow subgroup.

(a) Show that $j(P)$ is a p-Sylow subgroup of K.

Solution: Write $|G| = p^\alpha m$, $|N| = p^\gamma \ell$, $|K| = p^\beta n$, where $p \nmid \ell, m, n$. Since $P \subset G$ is a p-Sylow subgroup, we have $|P| = p^\alpha$. Note also that $K \cong G/\iota(N)$, so $|G| = |K||N|$, so $\alpha = \beta + \gamma$.

Note that $j(P) = \frac{P\,\iota(N)}{\iota(N)} \cong \frac{P}{P\cap\iota(N)}$. Since $P \cap \iota(N) \leq P$, we have $|P \cap \iota(N)| = p^k$ for some k. Since $p^k = |P \cap \iota(N)| \mid |\iota(N)| = p^\gamma \ell$, we have $k \leq \gamma$, so $p^k \leq p^\gamma$. Thus,

$$|j(P)| = \frac{|P|}{|P \cap \iota(N)|} = \frac{p^\alpha}{p^k} \geq \frac{p^\alpha}{p^\gamma} = p^\beta.$$

Since $j(P) \leq K$ is a p-group with $|j(P)| \geq p^\beta$, it follows that $|j(P)| = p^\beta$, meaning that $j(P)$ is a p-Sylow subgroup of K.

(b) If P_1, P_2 are two p-Sylow subgroups of G with $j(P_1) = j(P_2)$, show that there exists $n \in N$ with $i(n)P_2 i(n)^{-1} = P_1$. (Hint: apply a Sylow theorem to a subgroup of G.)

Solution: Write $|G| = p^\alpha m$, $|N| = p^\gamma \ell$, where $p \nmid \ell, m$. Since $P_1, P_2 \subset G$ are p-Sylow subgroups, we have $|P_1| = |P_2| = p^\alpha$.

Consider $\iota(N)P_1 \leq G$. The argument in part (a) shows that $|P_1 \cap \iota(N)| = p^\gamma$, so

$$|\iota(N)P_1| = \frac{|\iota(N)||P_1|}{|P_1 \cap \iota(N)|} = \frac{p^\gamma \ell \cdot p^\alpha}{p^\gamma} = p^\alpha \ell.$$

Thus, P_1 is a p-Sylow subgroup of $\iota(N)P_1$.

Note that $P_2 \leq \iota(N)P_1$. (If $p_2 \in P_2$, then $j(p_2) \in j(P_2) = j(P_1)$, so $j(p_2) = j(p_1)$ for some $p_1 \in P_1$, so $p_2 = \iota(n)p_1$ for some $n \in N$.) Thus, P_2 is a Sylow subgroup of $\iota(N)P_1$.

Therefore, by the Sylow Theorems, P_1 and P_2 are conjugate in $\iota(N)P_1$, so that

$$P_2 = \iota(n)p_1\, P_1\, (\iota(n)p_1)^{-1} = \iota(n)P_1\iota(n)^{-1}$$

for some $n \in N$.

8. Let A be a commutative ring, and M an A-module.

(a) Define what it means to say that M is A-flat, and prove that $\mathbb{Q}$ is a flat $\mathbb{Z}$-module that is not projective.

Solution: An A-module M is *A-flat* iff the right-exact functor $- \otimes_A M$ is exact. That is, every injective map $\psi\colon L' \to L$ has $\psi \otimes \mathrm{Id}\colon L' \otimes_A M \to L \otimes_A M$ injective.

Since $\mathbb{Q} = \mathbb{Z}_{(0)}$ is a localization of $\mathbb{Z}$, it is a flat $\mathbb{Z}$-module.

Suppose for the sake of contradiction that $\mathbb{Q}$ were a projective $\mathbb{Z}$-module. Then $\mathbb{Q} \oplus M = F$ for some $\mathbb{Z}$-module M and some free $\mathbb{Z}$-module F.

Let $A \subset F$ be a $\mathbb{Z}$-basis for F. Note that if $f = \sum k_i a_i$ for $k_i \in \mathbb{Z}$, $a_i \in A$ has $f \in nF$, then $n \mid k_i$ for each k_i. Thus, if $f \in \bigcap_{n=1}^{\infty} nF$, then each k_i has infinitely many divisors, so each $k_i = 0$, so $f = 0$. Therefore,

$$\bigcap_{n=1}^{\infty} n(\mathbb{Q} \oplus M) = \bigcap_{n=1}^{\infty} nF = 0.$$

But since $(1, 0) = n(1/n, 0) \in n(\mathbb{Q} \oplus M)$ for each $n \geq 1$, we have $(1, 0) \in \bigcap_{n=1}^{\infty} n(\mathbb{Q} \oplus M)$. Contradiction.

8. Let A be a commutative ring, and M an A-module.

(b) Prove that M is flat if and only if $\mathrm{Tor}_1^A(M, N) = 0$ for all A-modules N.

Solution: ($\Longrightarrow$) Suppose M is flat. Let N be an A-module, and let $P_* \to N \to 0$ be a projective resolution of N. Since M is flat, the tensored sequence

$$\cdots \to P_1 \otimes_A M \to P_0 \otimes_A M \to N \otimes_A M \to 0$$

is exact, hence has zero homology. That is, $\mathrm{Tor}_n^A(M, N) = 0$ for all $n \geq 1$.

($\Longleftarrow$) Suppose $\mathrm{Tor}_1^A(M, N) = 0$ for all A-modules N. Let $0 \to L' \to L \to L'' \to 0$ be a short exact sequence. Applying the Tor exact sequence gives

$$\cdots \to \mathrm{Tor}_1^A(M, L'') \to M \otimes_A L' \to M \otimes_A L \to M \otimes_A L'' \to 0. \qquad (ast)$$

By hypothesis $\mathrm{Tor}_1^A(M, L'') = 0$, so the sequence $(*)$ is short exact. Thus, the functor $M \otimes_A -$ is (left) exact, so M is flat.

(c) Prove that if $0 \to M' \to M \to M'' \to 0$ is a short exact sequence of A-modules and M' and M'' are A-flat, then so is M.

Solution: Let N be an A-module. Applying the long exact Tor sequence gives

$$\cdots \to \mathrm{Tor}_1^A(M', N) \to \mathrm{Tor}_1^A(M, N) \to \mathrm{Tor}_1^A(M'', N) \to \cdots$$

If M' and M'' are A-flat, then by part (b), we have $\mathrm{Tor}_1^A(M', N) = \mathrm{Tor}_1^A(M'', N) = 0$. Thus, $\mathrm{Tor}_1^A(M, N) = 0$. Since N is arbitrary, part (b) implies that M is A-flat.

10. Let $\pi\colon G \to \mathrm{GL}(V)$ be a finite-dimensional complex representation of a finite group G. On the respective spaces $\mathrm{Bil}(V)$ and $\mathrm{Hom}(V, V^*)$ of bilinear forms (on V) and linear maps, define left G-actions

$$(gB)(v, v') := B(g^{-1}v, g^{-1}v) \quad \text{and} \quad (gT)(v) = T(g^{-1}v) \circ \pi(g^{-1}).$$

(a) Prove that the natural linear map $\mathrm{Bil}(V) \to \mathrm{Hom}(V, V^*)$ defined by $B \mapsto (v \mapsto B(v, \cdot))$ is an isomorphism as well as G-equivariant.

Solution: Let $\varphi\colon \mathrm{Bil}(V) \to \mathrm{Hom}(V, V^*)$ denote $\varphi(B) = [v \mapsto B(v, \cdot)]$.

Injective: If $\varphi(B) = 0$, then $B(v, \cdot) = 0$ for all $v \in V$, so $B(v, w) = 0$ for all $v, w \in V$, meaning that $B = 0$.

Surjective: Let $A \in \mathrm{Hom}(V, V^*)$. Define $B \in \mathrm{Bil}(V)$ via $B(v, w) := (Av)(w)$. Then $\varphi(B)(v) = B(v, \cdot) = Av$ for all $v \in V$, so $\varphi(B) = A$.

G-equivariant: Let $B \in \mathrm{Bil}(V)$. Let $v, w \in V$. Note that by definition,

$$\varphi(gB)(v) = (gB)(v, \cdot) = B(g^{-1}v, g^{-1}\cdot)$$

and

$$[g\varphi(B)](v) = \varphi(B)(g^{-1}v) \circ \pi(g^{-1}) = B(g^{-1}v, \cdot) \circ \pi(g^{-1}).$$

Thus,

$$\varphi(gB)(v)(w) = B(g^{-1}v, g^{-1}w) = B(g^{-1}v, \cdot) \circ \pi(g^{-1})(w) = [g\varphi(B)](v)(w),$$

which shows that $\varphi(gB) = g\varphi(B)$.

10. Let $\pi\colon G \to \mathrm{GL}(V)$ be a finite-dimensional complex representation of a finite group G. On the respective spaces $\mathrm{Bil}(V)$ and $\mathrm{Hom}(V, V^*)$ of bilinear forms (on V) and linear maps, define left G-actions

$$(gB)(v, v') := B(g^{-1}v, g^{-1}v') \quad \text{and} \quad (gT)(v) = T(g^{-1}v) \circ \pi(g^{-1}).$$

(b) Prove that $\mathrm{Hom}_{\mathbb{C}[G]}(V, V^*) \neq 0$ if and only if there exists a nonzero bilinear form $B\colon V \times V \to \mathbb{C}$ satisfying $B(g(v), g(v')) = B(v, v')$ for all $g \in G$ and $v, v' \in V$, and deduce that if V is irreducible then such a nonzero B exists if and only if the character of π is $\mathbb{R}$-valued.

Solution: We first show that $\mathrm{Hom}_{\mathbb{C}[G]}(V, V^*) \neq 0$ iff there exists $B \in \mathrm{Bil}(V)$, $B \neq 0$ with $gB = B$.

($\Longrightarrow$) Suppose $\mathrm{Hom}_{\mathbb{C}[G]}(V, V^*) \neq 0$. Let $A \in \mathrm{Hom}_{\mathbb{C}[G]}(V, V^*)$, $A \neq 0$. Define $B \in \mathrm{Bil}(V)$ via $B(v, w) := (Av)(w)$. Then

$$B(gv, gw) = [A(gv)](gw) = (gAv)(gw) = (Av)(w) = B(v, w).$$

($\Longleftarrow$) Suppose there exists $B \in \mathrm{Bil}(V)$ with $B \neq 0$ and $gB = B$. Define $A\colon V \to V^*$ by $(Av)(w) := B(v, w)$. Then

$$[A(gv)](w) = B(gv, w) = B(v, g^{-1}w) = (Av)(g^{-1}w) = (gAv)(w),$$

so we have $A \in \mathrm{Hom}_{\mathbb{C}[G]}(V, V^*)$.

Suppose $\pi\colon G \to \mathrm{GL}(V)$ is irreducible. Let χ denote the character of π. We will show that $\mathrm{Hom}_{\mathbb{C}[G]}(V, V^*) \neq 0$ iff χ is $\mathbb{R}$-valued.

($\Longrightarrow$) Suppose $\mathrm{Hom}_{\mathbb{C}[G]}(V, V^*) \neq 0$. By Schur's Lemma, it follows that $V \cong V^*$ as representations. Since the character of V^* is $\overline{\chi}$, it follows that $\chi = \overline{\chi}$. Thus, χ is $\mathbb{R}$-valued.

($\Longleftarrow$) Suppose χ is $\mathbb{R}$-valued. Since $\dim_{\mathbb{C}}(\mathrm{Hom}_{\mathbb{C}[G]}(V, V^*)) = \langle \chi, \overline{\chi} \rangle$, we have

$$\begin{aligned}
\mathrm{Hom}_{\mathbb{C}[G]}(V, V^*) \neq 0 &\iff \dim_{\mathbb{C}}(\mathrm{Hom}_{\mathbb{C}[G]}(V, V^*)) \neq 0 \\
&\iff \langle \chi, \overline{\chi} \rangle \neq 0 \\
&\iff \frac{1}{|G|} \sum_{g \in G} \chi(g)^2 \neq 0.
\end{aligned}$$

Since χ is irreducible, the orthogonality relations imply that

$$\frac{1}{|G|} \sum_{g \in G} |\chi(g)|^2 = 1.$$

Since χ is $\mathbb{R}$-valued, we have

$$\frac{1}{|G|} \sum_{g \in G} \chi(g)^2 = 1 \neq 0.$$

Thus, $\mathrm{Hom}_{\mathbb{C}[G]}(V, V^*) \neq 0$.