

Mathematics 100C Final Exam Practice Problems

Instructions: The Final Exam is **Wednesday 14 June 2023, 11:30am-2:30pm (US Pacific time)**. It will be held in Warren Lecture Hall 2204, where we usually meet for lecture. No notes or calculators are allowed. This practice worksheet is to help you study for the Final Exam, which will cover the entire course. Specifically, the **Final will cover: finite fields; Galois theory (including Kummer theory); Noetherian rings, integer matrices, finitely generated abelian groups; representation theory**. Because you have already had much practice with finite fields and Galois theory, the practice worksheet focuses on the latter topics. However, the final will indeed cover the entire course, so do not forget to review the other topics. Note also that inclusion of a topic on this sheet does not guarantee that a similar problem will appear on the exam, nor does exclusion of a topic from this sheet imply that that topic will not be on the exam.

1. For a permutation $\sigma \in S_n$, let $f(\sigma)$ denote the number of fixed points of σ . Prove that $\sum_{\sigma \in S_n} f(\sigma)^2 = 2n!$. **Hint:** Let S_n act on $\mathbf{C}^n$ by permuting the coordinates, and let χ be the character of this representation. Compute $\langle \chi, \chi \rangle$ in two different ways.

Proof. Let U denote the standard representation of S_n on $\mathbf{C}^{n-1}$, and V denote the permutation representation of S_n on $\mathbf{C}^n$. Then $V = U \oplus \mathbf{1}$ is the decomposition into irreducibles. Thus, if χ is the character of the representation of S_n on V , then $\langle \chi, \chi \rangle = 2$. On the other hand, if $\sigma \in S_n$, then $\chi(\sigma) = f(\sigma)$. The claim follows. $\square$

2. Prove that the only 1-dimensional representations of the symmetric group S_n are the trivial representation and the sign representation.

Proof. First observe that every permutation of the form (ab) is conjugate to (12) . Thus if $\rho : S_n \rightarrow \mathbf{C}^\times$ is a homomorphism, then ρ takes the same values on all these permutations. Because $(12)^2 = 1$, we have $\rho((12)) = \pm 1$. In case it is 1, then ρ is trivial, because the permutations (ab) generate S_n . In case $\rho((12)) = -1$, then ρ must be the sign representation, again because the permutations (ab) generate S_n . $\square$

3. Define explicitly the n irreducible representations of the group C_n .

Proof. The irreducible representations of an abelian group are always one-dimensional. Thus we must determine the homomorphisms $C_n \rightarrow \mathbf{C}^\times$. If ρ is such a homomorphism, then $\rho(1+n\mathbf{Z})$ must be an n^{th} root of unity, and ρ is uniquely determined by such a $\zeta \in \mu_n$. Hence the irreps are ρ_k , $k \in \mathbf{Z}/n\mathbf{Z}$, where $\rho_k(a+n\mathbf{Z}) = e^{2\pi i a k/n}$. $\square$

4. Let C_n act on $\mathbf{C}^2$ by $k+n\mathbf{Z} \mapsto \begin{pmatrix} \cos(\theta_k) & -\sin(\theta_k) \\ \sin(\theta_k) & \cos(\theta_k) \end{pmatrix}$, where $\theta_k = 2\pi k/n$. Decompose this representation into irreducibles.

Proof. Let ρ be the representation given. Let $b_{-1} = (1, i)^t$ and $b_1 = (1, -i)^t$. Then $\rho(k+n\mathbf{Z})b_{-1} = e^{-2\pi i k/n}b_{-1}$ and $\rho(k+n\mathbf{Z})b_1 = e^{2\pi i k/n}b_1$. Thus $\mathbf{C}^2 = \mathbf{C}b_{-1} \oplus \mathbf{C}b_1$ and ρ is a sum of the representations ρ_{-1} and ρ_1 , in the notation of the previous exercise. $\square$

5. Let G be a finite group. Suppose the character table of G is given by an array A , so that the complex number A_{ij} is $\chi_i(g_j)$, where χ_i is the i^{th} irreducible representation of G and g_j is a representative of the j^{th} conjugacy class in G . (We arbitrarily order the irreps and the conjugacy classes.) Let c_j be the size of the j^{th} conjugacy class.

- (a) Define a matrix T as $T_{ij} = \left(\frac{c_j}{|G|}\right)^{1/2} A_{ij}$. Prove that $TT^* = 1$.
- (b) Deduce that the columns, and not just the rows, of the character table of G are orthogonal.

Proof. The first point follows exactly from the orthonormality of the characters of the irreps. For the second point, from $TT^* = 1$, we obtain $T^*T = 1$. This new relation gives that the columns of the character table are orthogonal. $\square$

6. Suppose G is a finite group, that has a normal subgroup N of index 2. Suppose moreover that N is abelian. Prove that every irreducible representation of G has dimension either 1 or 2. **Hint:** Let V be the space of an irreducible representation of G . Restrict the action of G on V to N to find an eigenvector v for the action of N . If $\sigma \in G \setminus N$, let $w = \sigma(v)$ and prove that $\mathbf{C}v + \mathbf{C}w$ is G -stable.

Proof. One proceeds exactly as in the hint. Because N is abelian, it has a simultaneous eigenvector v . Let $w = \sigma(v)$. Then if $n \in N$, $nw = n\sigma v = \sigma n'v = \lambda\sigma(v)$ for some $\lambda \in \mathbf{C}^\times$. Here we are using that N is normal to write $n\sigma = \sigma n'$. Thus $\mathbf{C}v + \mathbf{C}w$ is stable by N . Because $\sigma^2 \in N$, it is also easy to see that it is stable by σ . Thus $\mathbf{C}v + \mathbf{C}w$ is stable by G . Thus every G -representation has a subspace of dimension at most two that is G -stable. Thus all irreps have dimension 1 or 2 as claimed. $\square$

7. Suppose N is a normal subgroup of G , ρ' an irreducible representation of G/N , and $\rho = \rho' \circ \pi$, where $\pi : G \rightarrow G/N$ is the quotient map. Prove that ρ is irreducible.

Proof. This is immediate from the definitions. $\square$

8. Suppose $\rho : G \rightarrow \text{GL}(V)$ is a representation, and $\dim(V) = d$.
- (a) Let χ be the character of ρ . Prove $|\chi(g)| \leq d$, and $\chi(g) = d$ if and only if $\rho(g) = 1$.
- (b) Explain, using the first part, how one can determine if a finite group is simple by looking at its character table.

Proof. For the first part, we proved that $\chi(g)$ is a sum of d roots of unity, $\chi(g) = \lambda_1 + \cdots + \lambda_d$ where all λ_j are roots of unity. Thus $|\chi(g)| \leq d$ by the triangle inequality. Moreover, by considering (say) real parts, one sees $\chi(g) = d$ if and only if all $\lambda_j = 1$. Because $\rho(g)$ is diagonalizable and the λ_j are the eigenvalues of $\rho(g)$, there are all equal to 1 if and only if $\rho(g) = 1$.

By the previous problem, one sees that a group is simple if and only if every nontrivial irrep is faithful. Indeed, if G is simple, then every nontrivial irrep must be faithful, because there are no proper normal subgroups. And if G is not simple, then it has a proper normal subgroup N , and then the quotient group G/N has a nontrivial irrep, which can be considered an irrep of G by the previous problem. So, to detect if G is simple, we just must see if $\chi(g) = \chi(1)$ for any irreducible character χ and $g \neq 1$: If there is a nontrivial irrep χ for which $\chi(g) = \chi(1)$ for some $g \neq 1$, then G is not simple, and if $\chi(g) \neq \chi(1)$ for all $g \neq 1$ and all nontrivial irreducible characters χ , then G is simple. $\square$

9. Suppose $\rho : G \rightarrow \text{GL}(V)$ is an irreducible representation, and $\langle \cdot, \cdot \rangle_j$ for $j = 1, 2$ are G -invariant Hermitian forms on V . Suppose $\langle \cdot, \cdot \rangle_1$ is positive definite. Prove that there exists $\lambda \in \mathbf{C}$ so that $\langle v, w \rangle_2 = \lambda \langle v, w \rangle_1$ for all $v, w \in V$. **Hint:** For $v \in V$, consider the linear map $V \rightarrow \mathbf{C}$

given by $x \mapsto \langle v, x \rangle_2$. There exists a unique vector $A(v) \in V$ so that this linear map is $\langle A(v), x \rangle_1$. Prove that $v \mapsto A(v)$ is linear and G -equivariant, then apply Schur's lemma.

Proof. Exactly as in the hint, one checks immediately that $A(v) : V \rightarrow V$ is $\mathbf{C}$ -linear and G -equivariant. Thus by Schur's lemma, there exists $\lambda \in \mathbf{C}$ so that $A(v) = \lambda v$ for all $v \in V$. The problem follows. $\square$

10. Suppose $\chi : G \rightarrow \mathbf{C}^\times$ is a homomorphism, and $\rho : G \rightarrow \mathrm{GL}(V)$ a representation. Let $V(\chi)$ be the vector space V , but with G action given as $g \cdot v = \chi(g)\rho(g)(v)$. Prove that if ρ is irreducible, then so is the G -action on $V(\chi)$.

Proof. Let χ_ρ be the character of ρ . Then the character of the new representation is $g \mapsto \chi_\rho(g)\chi(g)$. But then $\langle \chi_\rho\chi, \chi_\rho\chi \rangle = \langle \chi, \chi \rangle = 1$, so the new representation is irreducible.

One can also easily do this problem directly, without using characters. $\square$

11. Suppose G is a finite group. Recall that a *class function* $\varphi : G \rightarrow \mathbf{C}$ is a function that is constant on conjugacy classes.

(a) Suppose φ is a class function. Verify that $\varphi(g) = \sum_{\chi_i} \langle \chi_i, \varphi \rangle \chi_i$, where the sum is over the characters of the irreducible representations of G .

(b) Suppose now that $G = C_n$. Then a class function is any function $\varphi : \mathbf{Z}/n\mathbf{Z} \rightarrow \mathbf{C}$. Write out explicitly the identity $\varphi(g) = \sum_{\chi_i} \langle \chi_i, \varphi \rangle \chi_i$ in this case. The complex numbers $\langle \chi_i, \varphi \rangle$ in this case are called the Fourier coefficients of φ , and this identity can be thought of as part of the theory of the *finite Fourier transform*.

Proof. Because the χ_i are a basis of the space of class functions, we can write $\varphi = \sum_j a_j \chi_j$ for some complex numbers a_j . Taking the inner product with χ_j gives $a_j = \langle \chi_j, \varphi \rangle$.

For the second part, suppose $\phi : C_n \rightarrow \mathbf{C}$ is an arbitrary function. Let χ_j be the character of ρ_j , where ρ_j was defined in a previous problem. Then $\chi_j(k + n\mathbf{Z}) = e^{2\pi i j k / n}$. Consequently,

$$\widehat{\varphi}(j) := \langle \chi_j, \varphi \rangle = \frac{1}{n} \sum_{k \in \mathbf{Z}/n} e^{-2\pi i \sqrt{-1} j k / n} \varphi(k)$$

and the Fourier identity says $\varphi = \sum_j \widehat{\varphi}(j) \chi_j$. $\square$

12. Make the character tables for C_4 and K_4 , the cyclic group of order 4 and the Klein 4 group.

Proof. Of course, the tables you come up with depend upon exactly how you order the elements of these groups and the irreps. Here is one possibility. The first table is for K_4 and the second table for C_4 .

*	(1, 1)	(1, -1)	(-1, 1)	(-1, -1)
χ_1	1	1	1	1
χ_2	1	1	-1	-1
χ_3	1	-1	1	-1
χ_4	1	-1	-1	1

*	$0 + 4\mathbf{Z}$	$1 + 4\mathbf{Z}$	$2 + 4\mathbf{Z}$	$3 + 4\mathbf{Z}$
χ_1	1	1	1	1
χ_2	1	i	-1	$-i$
χ_3	1	-1	1	-1
χ_4	1	$-i$	-1	i

□

13. Let $R = F[t]$ for a field F , and S a subring of R that contains F and is strictly bigger than F . Prove that R is a finitely generated S module.

Proof. . Because S is strictly bigger than F and contains F , there is some monic polynomial $f(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_0 \in S$. We claim that R is generated as an S -module by the elements $1, t, t^2, \dots, t^{n-1}$. Let $M = S1 + St + \cdots + St^{n-1} \subseteq R$. We wish to prove $M = R$.

Thus suppose $g(t) \in R$. If $\deg(g) < n$, then $g \in M$. If $\deg(g) \geq n$, write $g = qf + r$, with $q \in F[t]$ and $\deg(r) < n$. By induction, $q \in M$ and $r \in M$. Thus $g \in M$ as well. □

14. Suppose $v = (v_1, \dots, v_n) \in \mathbf{Z}^n$ is such that the v_j have no common divisor. Prove that v can be extended to a basis of $\mathbf{Z}^n$.

Proof. By our theorem on diagonalization of matrices, there is $P \in \text{GL}_n(\mathbf{Z})$ so that $vP = (1, 0, 0, \dots, 0)$. Thus if $e_1, \dots, e_n$ is the standard basis of $\mathbf{Z}^n$, then $e_1P^{-1}, \dots, e_nP^{-1}$ is also a basis, but this basis includes v . □

15. Suppose $A \in M_n(\mathbf{Z})$ has $\det(A) = N$. Suppose $v \in N\mathbf{Z}^n$. Prove that there exists $w \in \mathbf{Z}^n$ so that $Aw = v$.

Proof. If $N = 0$, the conclusion is clear. Thus suppose $N \neq 0$. Then by a homework question, $\mathbf{Z}^n/A\mathbf{Z}^n$ is a finite abelian group of size N . Write $v = Nv_1$ with $v_1 \in \mathbf{Z}^n$. Then by Lagrange's theorem, $Nv_1 \equiv 0$ in $\mathbf{Z}^n/A\mathbf{Z}^n$, so v is in the image of A , as desired. □

16. Let V be a finite dimensional F vector space, and $T : V \rightarrow V$ a linear operator. Suppose $p(x) \in F[x]$ is irreducible of degree d , and $p(T) = 0$ on V . Prove that d divides $\dim(V)$.

Proof. Let $E = F[x]/(p(x))$. Then E is a field, of degree d over F . The hypothesis of the question implies that V is a finitely generated E -module. Thus $V \approx E^r$ for some $r \geq 1$, so $\dim(V) = dr$ is divisible by d . □

17. Let F be a field, V a finite dimensional F vector space, and $N : V \rightarrow V$ a linear map. One says that N is *nilpotent* if $N^k = 0$ for some positive integer k .

(a) Suppose the matrix of N is upper triangular, with 0's along the diagonal. Prove that N is nilpotent.

(b) Let V_r be the $r \times r$ matrix with 1's along the super diagonal and 0's elsewhere. That is, $V_{i,i+1} = 1$ for $i = 1, 2, \dots, r-1$ and the other matrix entries $V_{ij} = 0$. Prove that if N is nilpotent, then there is a basis of V so that in this basis, the matrix of N is block diagonal, with blocks of the form V_r for various integers r . **Hint:** Consider V as a module for $k[x]$, and use the structure theorem for modules over this ring that we proved.

Proof. For the first part, let $b_1, \dots, b_r$ be the basis that makes N upper triangular, with 0's along the diagonal. Set $V_j = \text{Span}\{b_1, \dots, b_j\}$, and $V_0 = \{0\}$. Then clearly N maps V_{j+1} to V_j for each j . Thus $N^r = 0$. This proves the first part.

For the second part, we can write $V \simeq k[x]/(f_1(x)) \oplus \cdots \oplus k[x]/(f_m(x))$ for polynomials $p_j(x)$, with the action of N on V corresponding to multiplication by x . Because $N^k = 0$ on V for some $k > 0$, we see $f_j(x) | x^k$ for all j . Thus $f_j(x) = x^{a_j}$ for some positive integers a_j . Taking the basis $x^{a_j-1}, x^{a_j-2}, \dots, x, 1$ of $k[x]/(x^{a_j})$, one sees that $k[x]/(x^{a_j})$ gives an $a_j \times a_j$ block of the type described in the problem. □

18. Let $G = C_{10} \times C_5 \times C_{100}$. How many elements $x \in G$ are there with $x^2 = 1$?

Proof. There are $2 \times 1 \times 2 = 4$ such elements. $\square$

19. Suppose $m = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbf{Z})$ has $\gcd(a, b, c, d) = u$ and $|\det(m)| = v = u^2 v_1$ for some positive integers u, v_1 . Let $P, Q \in \text{GL}_2(\mathbf{Z})$ be such that $m' := QmP^{-1} = \text{diag}(a_1, a_2)$ with $a_1, a_2 > 0$ and $a_1 | a_2$. What are a_1 and a_2 ?

Proof. Observe that if u divides a, b, c, d , then $u^2 | \det(m)$ so indeed $|\det(m)| = u^2 v_1$ for some positive integer v_1 . Now, the multiplication by P, Q does not change the gcd of the entries, nor does it change the absolute value of the determinant. Thus $a_1 = u$ and $a_2 = uv_1$. $\square$

20. Let G be the abelian group generated by elements x, y with $x^{20} = 1$, $y^{30} = 1$, and $x^2 = y^3$.

(a) Write a presentation matrix for the group G .

(b) Describe G explicitly as a product of cyclic groups.

Proof. A presentation matrix for G is

$$A = \begin{pmatrix} 20 & 0 & 2 \\ 0 & 30 & -3 \end{pmatrix}.$$

That is, $G \simeq \mathbf{Z}^2 / A\mathbf{Z}^2$.

Doing some column operations to A , one gets the matrix $A' = \begin{pmatrix} 0 & 20 & 2 \\ 0 & 0 & -3 \end{pmatrix}$. We can delete the first column, to obtain $A'' = \begin{pmatrix} 20 & 2 \\ 0 & -3 \end{pmatrix}$, and $G \simeq \mathbf{Z}^2 / A''\mathbf{Z}^2$. By the previous problem, $A'' = PA'''Q$ with $P, Q \in \text{GL}_2(\mathbf{Z})$ and $A''' = \text{diag}(1, 60)$. Thus $G \simeq C_{60}$. $\square$