

Mathematics 100C Exam 1 Practice Problems

Instructions: Exam 1 is Friday April 21. It will be an in class exam, 50 minutes long. No notes or calculators are allowed. This practice worksheet is to help you study for Exam 1. Anything discussed up to and including the material in lecture on Friday April 14 is fair game for the exam. Note 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. Fix a prime number p . For an integer $k \geq 1$, let $H_k(p)$ denote the number of irreducible monic polynomials of degree k over $\mathbf{F}_p$. For example, $H_1(p) = p$.
 - (a) Find a formula that relates the $H_k(p)$ for different k , and which allows you to determine the numbers $H_k(p)$ inductively.
 - (b) Give a simple closed formula for $H_\ell(p)$ where ℓ is a prime number. Note that ℓ might be equal to p , and it also might not be equal to p .
 - (c) Compute $H_4(3)$.

Proof. One has $\sum_{k|r} kH_k(p) = p^r$, by considering the prime factorization of $x^{p^r} - x$ over $\mathbf{F}_p$. Consequently, if ℓ is prime, $H_\ell(p) = (p^\ell - p)/\ell$.

One has $H_2(3) = (3^2 - 3)/2 = 3$, and $3 + 2 * H_2(3) + 4 * H_4(3) = 81$, so $H_4(3) = (81 - 9)/4 = 18$. $\square$

2. Prove that, if K is a finite field, then there exists a maximal ideal M in $\mathbf{Z}[x]$ so that $\mathbf{Z}[x]/M$ is isomorphic to K .

Proof. This follows directly from the fact that K has a primitive element over $\mathbf{F}_p$. Suppose $K = \mathbf{F}_q$ with $q = p^r$. Concretely, let $f(x) \in \mathbf{Z}[x]$ be a monic polynomial of degree r whose reduction modulo p is irreducible (such f exists because K has a primitive element). Then we can take $M = (p, f(x))$. $\square$

3. Suppose F is a finite field of order p a prime, and K is a finite extension of F of degree ℓ , where ℓ is prime. How many primitive elements are there for K over F ? How about if the degree of K over F is ℓ^n , where again ℓ is prime?

Proof. Let F_j denote the field of order p^{ℓ^j} . Note that we have

$$F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots F_n = K$$

and that F_j has degree ℓ^j over F . Moreover, every subfield E of K is an F_j . An element $\gamma \in K$ is primitive over F if and only if it is not in any subfield. Thus there are $p^{\ell^n} - p^{\ell^{n-1}}$ primitive elements for K over F . $\square$

4. This problem and the next develop some of the theory of so-called *cyclotomic polynomials*. This is an important topic, which we might not have time to cover in class, so I highly recommend that you do this problem and the next one. To get started, let $\zeta_n = e^{2\pi i/n} \in \mathbf{C}$. If a is an integer relatively prime to n , note that ζ_n^a is a primitive n^{th} root of unity, meaning that its order in the multiplicative group $\mathbf{C}^\times$ is exactly n . Define

$$\Phi_n(x) = \prod_{1 \leq a \leq n, (a,n)=1} (x - \zeta_n^a).$$

Note that the degree of $\Phi_n(x)$ is $\varphi(n)$.

- (a) Prove that $x^n - 1 = \prod_{d|n} \Phi_d(x)$. (Deduce also that $n = \sum_{d|n} \varphi(d)$).
- (b) Prove inductively that $\Phi_n(x)$ is monic with integral coefficients. **Hint:** Apply Gauss' Lemma.

Proof. The first part follows by observing every n^{th} root of unity has order some integer d where $d|n$. For the second part, we proceed by induction. (The base case is trivial.). Thus suppose one knows that all $\Phi_d(x)$ have integral coefficients for $d < n$. (It is clear that they are monic.). Then $\prod_{d|n, d < n} \Phi_d(x)$ is a monic integral polynomial that divides $x^n - 1$ in $\mathbf{C}[x]$, so it divides it in $\mathbf{Q}[x]$. Then, by Gauss' Lemma, it divides $x^n - 1$ in $\mathbf{Z}[x]$ as desired. $\square$

5. The purpose of this problem is to show the following theorem.

Theorem: The polynomial $\Phi_n(x) \in \mathbf{Q}[x]$ is irreducible. Consequently, $[\mathbf{Q}(\zeta_n) : \mathbf{Q}] = \varphi(n)$.

Proceed as follows:

- (a) Suppose $\Phi_n(x) = f(x)g(x)$ factors over $\mathbf{Q}$, with $f(x)$ irreducible. Remind yourself (using Gauss' Lemma), that you can assume f, g are monic with integral coefficients.
- (b) Let ζ be a primitive n^{th} root of unity that is a root of $f(x)$ in $\mathbf{C}$. Let p be an arbitrary prime that does not divide n . We will show that ζ^p is also a root of $f(x)$.
- (c) For the sake of contradiction, assume that ζ^p is a root of $g(x)$. Then ζ is a root of $g(x^p)$. Deduce that $g(x^p) = f(x)h(x)$ for some polynomial $h(x)$ with integral coefficients.
- (d) Reducing modulo p , obtain that $\overline{g(x)^p} = \overline{f(x)h(x)}$. Conclude that $\overline{f}, \overline{g}$ share a common factor in $\mathbf{F}_p[x]$.
- (e) Thus, $\Phi_n(x)$ and then $x^n - 1$ have a multiple roots modulo p . By considering the derivative of $x^n - 1$, see that this is a contradiction.
- (f) Consequently, if ζ is an arbitrary primitive n^{th} root of unity that is a root of $f(x)$, ζ^p is also a root of $f(x)$. Deduce that all ζ_n^a for $(a, n) = 1$ are roots of $f(x)$, so that $\Phi_n(x) = f(x)$ is irreducible.
- (g) Deduce the corollary that $[\mathbf{Q}(\zeta_n) : \mathbf{Q}] = \varphi(n)$.

Proof. Parts (a), (b), (c), (d) are clear. For part (e), one has $x(n x^{n-1}) - n(x^n - 1) = n$. Over $\mathbf{F}_p$, then, $x^n - 1$ and its derivative are relatively prime (because $p \nmid n$), so $x^n - 1$ has no multiple roots modulo p . For part (f), if ζ is a primitive n^{th} root of unity, then all other primitive n^{th} roots of unity are of the form ζ^a with a a product of primes that do not divide

n . Thus by the previous parts all primitive n^{th} roots of unity are roots of $f(x)$. Part (g) follows because the minimal polynomial of ζ_n is $\Phi_n(x)$, which has degree $\varphi(n)$. $\square$

6. This problem does not really concern what we've talked about in class this term, but it proves for you a formula for $\varphi(n)$ using ideas from 100B, and gives an application.
- (a) Recall that $\varphi(n)$ is the number of integers a with $1 \leq a \leq n$ and $(a, n) = 1$. Prove that $\varphi(n)$ is the size of the unit group $(\mathbf{Z}/n\mathbf{Z})^\times$.
 - (b) Suppose $n = p_1^{e_1} \cdots p_r^{e_r}$ is its prime factorization. Prove, using the CRT, that $\varphi(n) = \varphi(p_1^{e_1}) \cdots \varphi(p_r^{e_r})$.
 - (c) Prove that if p is prime, then $\varphi(p^e) = p^e - p^{e-1} = (1 - 1/p)p^e$.
 - (d) Find all integers n so that $\varphi(n) \leq 2$. Deduce (using the previous problem) all n^{th} roots of 1 that can be found in quadratic field extensions of $\mathbf{Q}$.

Proof. This is basically a direct application of the CRT, by observing that

$$\mathbf{Z}/n\mathbf{Z} \simeq (\mathbf{Z}/p_1^{e_1}) \times \cdots \times (\mathbf{Z}/p_r^{e_r})$$

and then taking units of both sides. For the last part, one finds the $n = 1, 2, 3, 4, 6$ are the only such n with $\varphi(n) \leq 2$. $\square$

7. Prove that $\mathbf{Q}(\zeta_n)$ is Galois over $\mathbf{Q}$ with Galois group identified with $(\mathbf{Z}/n\mathbf{Z})^\times$.

Proof. The element ζ_n is a primitive element for $K = \mathbf{Q}(\zeta_n)$ over $F = \mathbf{Q}$, and all roots of its minimal polynomial over F are in K . Thus, K is Galois over F . To compute the Galois group, note that if $\sigma \in \text{Gal}(K/F)$, then $\sigma(\zeta_n) = \zeta_n^a$ for some a relatively prime to n . Moreover, then, if ζ is an arbitrary primitive n^{th} root of unity, one has $\sigma(\zeta) = \zeta^a$. This gives a map of sets $\text{Gal}(K/F) \rightarrow (\mathbf{Z}/n\mathbf{Z})^\times$ sending σ to the class of a . It is easily seen that this map is a group isomorphism. $\square$

8. Set $K = \mathbf{Q}(\sqrt{2}, \sqrt{3})$ and $F = \mathbf{Q}$. Prove that K has degree four over F . Now, using the first main theorem of Galois theory, check that K is Galois over F . What is its Galois group? Using the second main theorem of Galois theory, explicitly classify the primitive elements γ of K over F . More precisely, if $\gamma = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$, with $a, b, c, d \in F$, for which a, b, c, d is γ a primitive element?

Proof. I will discuss this example in class on Monday April 17. $\square$

9. Suppose K/F is a finite extension of fields. Recall if $x \in K$, we defined $N_{K/F}(x)$, the norm of x , to be the determinant of the map $L_x : K \rightarrow K$ given by left multiplication by x . Now suppose F is a field of characteristic not 2, and K is a quadratic extension of F . Let $\sigma \in \text{Aut}(K/F)$ be the unique non-trivial element. Prove that $N_{K/F}(x) = x\sigma(x)$ as an identity of elements of K . **Note:** This formula generalizes widely.

Proof. Suppose $K = F(\sqrt{a})$, and $x = u + v\sqrt{a}$ is in K , with $u, v \in F$. On the one hand, you proved in an exercise last quarter, that $N_{K/F}(x) = u^2 - av^2$. On the other hand, $\sigma(x) = u - v\sqrt{a}$, so $x\sigma(x) = u^2 - av^2$. $\square$

10. Suppose F is a field of characteristic 0, and K is a finite Galois extension of F of degree n . Set $G = \text{Gal}(K/F)$. The purpose of this problem is to prove the following theorem.

Theorem For all $\gamma \in K$, $N_{K/F}(\gamma) = \prod_{\sigma \in G} \sigma(\gamma)$.

- (a) First suppose $\gamma \in K$ is a primitive element, with monic irreducible polynomial $f(x) \in F[x]$ of degree n . Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Using the basis $1, \gamma, \gamma^2, \dots, \gamma^{n-1}$ of K/F , find the matrix $m(\gamma)$ of L_γ in terms of the coefficients a_j .
- (b) Using the previous part, deduce that $N_{K/F}(\gamma) = (-1)^n a_0$. **Hint:** Compute the determinant of the $m(\gamma)$ by permuting the columns of $m(\gamma)$ in such a way that you get a lower triangular matrix, whose determinant can thus be easily computed. Determine also how permuting the columns changes the sign of the determinant.
- (c) Using the fact that K/F is Galois with Galois group G , observe that $f(x) = \prod_{\sigma \in G} (x - \sigma(\gamma))$. (The $\sigma(\gamma)$ are all distinct, because σ is determined by its action on γ ...)
- (d) Deduce that $a_0 = (-1)^n \prod_{\sigma \in G} \sigma(\gamma)$, which then implies the theorem in case γ is a primitive element.
- (e) One can now deduce the general case from this special case, in a couple different ways. If you'd like to know how, feel free to ask, and we can discuss it in office hours!

Proof. The matrix $m(\gamma)$ has, in the first $n-1$ columns, 1 in the $(j+1, j)$ entry, and 0's elsewhere. In the last column, the entries are $(-a_0, -a_1, \dots, -a_{n-1})^t$. Cyclically permuting the rows multiplies the determinant by $(-1)^{n-1}$, and the new (lower triangular) matrix has determinant $-a_0$. Thus $\det(m(\gamma)) = (-1)^n a_0$. The next part is clear.

For the final part, and also the fact that this formula generalizes to non-Galois extensions, feel free to talk to me in office hours. $\square$