Artwork Ig: `@itchyscabs` `@mimithemimo`

Professor Kenneth A. Ribet
December 16, 2020
3–6 PM

You have 180 minutes to work on the exam and 15 minutes to upload your work to `Gradescope`. You may consult the textbook, all the material on `bCourses`, the class `piazza` and your own notes. In case of questions, post a private note to instructors on `piazza`. Any clarifications or corrections that need to be promulgated will be added to a pinned post on `piazza`.

Not permitted: online searches, other uses of the internet, collaboration with other people (electronic or otherwise). Please act with honesty, integrity and respect for others.

Please do Problems 1–6 and either Problem 7 or Problem 8. Once you have selected the problem (8 or 7) that you will not do, write prominently in place of a solution to the problem "**I did not do this problem**."

Problem	1	2	3	4	5	6	7 or 8	Total
Points	6	6	4	6	5	6	7	40

In your work, you may use the following result:

> **Dirichlet's theorem on primes in an arithmetic progression.** *If a and m are relatively prime positive integers, there exist infinitely many prime numbers that are congruent to a modulo m.*

1a. Show that every group of order $n = 3 \cdot 17^2$ has a unique subgroup of index 3.

b. Are there groups of order n that are cyclic? abelian but not cyclic? non-abelian? Explain your reasoning carefully and cite concrete examples as needed.

2a. If G is a finite abelian group, show that there is a positive integer N so that G is isomorphic to a quotient of the group $(\mathbf{Z}/N\mathbf{Z})^*$.

b. Show that every finite abelian group is isomorphic to $\mathrm{Gal}(K/\mathbf{Q})$ for some Galois extension K of $\mathbf{Q}$.

3. According to an email that I received on Monday from a crank mathematician, "All existing irrational numbers seem to be algebraic constructions of constant Phi and 1." The writer intends Phi to be $\dfrac{1+\sqrt{5}}{2}$. Prove that p is not a perfect square in $\mathbf{Q}(\sqrt{5})$ if p is a prime different from 5.

4. Let K/F be a finite Galois extension, and let p be a prime number. Show that there is an intermediate field E in the extension $(K \supseteq E \supseteq F)$ so that K/E has p-power degree and E/F has degree prime to p. If E and E' are two fields with these properties, show that there is an isomorphism $\sigma : E \xrightarrow{\sim} E'$ whose restriction to F is the identity.

5. Let G be a finite group, and let Z be the center of G. For each $g \in G$, let $i_g = (G : Z_g)$, where Z_g is the centralizer of g. Thus, for example, $i_g = 1$ if and only if g lies in Z. Consider the set of numbers $\{\, i_g \,|\, g \notin Z \,\}$. Show that every integer that divides all of these numbers divides $|Z|$.

6. Let G be a finite group all of whose proper subgroups are abelian. Suppose that N is a proper normal subgroup of G that is not contained in the center of G. Show that N is contained in a normal subgroup of G whose index in G is prime.

Here is an outline of the proof. Your job is to write a full proof, perhaps using some or all of the steps from the outline.

> Let M be maximal among the proper normal subgroups of G that contain N. The centralizer $C_G(N)$ of N is a proper normal subgroup of G that contains M and therefore must be M. It follows that $M = C_G(M)$. Because all proper subgroups of G are abelian, M is a maximal proper subgroup of G (and not just a maximal proper normal subgroup of G). Thus G/M is cyclic of prime order, so that $(G : M)$ is prime.

7. This problem concerns finite fields:

a. As a warmup, list all irreducible polynomials of degree 3 over the field with two elements.

Let $\mathbf{F}$ be a finite field, and let $q = |\mathbf{F}|$. Let ℓ be a prime number.

b. How do we know that there are fields K containing $\mathbf{F}$ for which $[K : \mathbf{F}] = \ell$?

c. If K_1 and K_2 are fields as in part (b), prove that there is an isomorphisms $\sigma : K_1 \xrightarrow{\sim} K_2$ that is the identity on $\mathbf{F}$. If σ is one such isomorphism, how do we obtain the others? How many isomorphisms are there?

d. Show that every irreducible polynomial $f \in \mathbf{F}[X]$ of degree ℓ splits completely over K, if K is an extension of $\mathbf{F}$ of degree ℓ.

e. Show that the number of monic irreducible polynomials $f \in \mathbf{F}[X]$ of degree ℓ is $\dfrac{1}{\ell}(q^\ell - q)$.

8. On the last homework, you proved by two different methods that $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/2}$ when p is an odd prime. In other words, you proved that $\left(\frac{2}{p}\right) = 1$ if $p \equiv \pm 1 \bmod 8$ and $\left(\frac{2}{p}\right) = -1$ if $p \equiv \pm 5 \bmod 8$. This problem presents yet another proof.

Recall that if a is an integer and n is an odd positive integer, we defined the Jacobi symbol by the formula

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{t} \left(\frac{a}{p_i}\right)$$

if $n = p_1 \cdots p_t$ and the p_i are odd prime numbers. The value of $\left(\frac{a}{n}\right)$ depends only on a modulo n. You already know:

$$\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2} \text{ if } n \text{ is an odd positive integer,}$$
$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = (-1)^{\frac{n-1}{2}\frac{m-1}{2}} \text{ if } n \text{ and } m \text{ are relatively prime positive integers.}$$

a. If n and m are odd positive relatively prime integers, use the formulas just above to show that

$$\left(\frac{m}{n}\right) = \left(\frac{(-1)^{(n-1)/2}n}{m}\right).$$

b. Let p be an odd prime, and set $e = (-1)^{(p-1)/2} = \pm 1$, $a = (p+e)/2$. Prove that a is odd and that $a \equiv 1 \bmod 4$ if and only if $p \equiv 1$ or $3 \bmod 8$.

c. Show that

$$\left(\frac{2e}{p}\right) = \left(\frac{2e+2p}{p}\right) = \left(\frac{4a}{p}\right) = \left(\frac{a}{p}\right).$$

d. Show that $ep = 2ea - 1$ and thus that

$$\left(\frac{a}{p}\right) = \left(\frac{(-1)^{(p-1)/2}p}{a}\right) = \left(\frac{ep}{a}\right) = \left(\frac{2ea-1}{a}\right) = \left(\frac{-1}{a}\right).$$

e. Deduce that

$$(-1)^{(p-1)/2}\left(\frac{2}{p}\right) = \left(\frac{-1}{a}\right).$$

f. Compute the value of $\left(\frac{2}{p}\right)$ by computing the values of $(-1)^{(p-1)/2}$ and $\left(\frac{-1}{a}\right)$ in each of the four cases $p \equiv 1, 3, 5, 7 \bmod 8$.

9. To finish, please copy and sign:

> "*As a member of the UC Berkeley community, I acted with honesty, integrity, and respect for others during this exam. The work that I am uploading is my own work. I did not collaborate with or contact anyone during the exam. I did not obtain solutions from* `chegg.com` *or other sites. I adhered to all instructions for this examination.*"