Math 250A

PROFESSOR KENNETH A. RIBET

Final Exam

December 15, 2015

8:00–11:00PM, 247 Cory Hall

Please write your NAME clearly:

Please put away all books, calculators, cell phones and other devices. You may consult a single two-sided sheet of notes. Please write carefully and clearly in *complete sentences.*

Problem	Your score	Possible points
1		5 points
2		5 points
3		5 points
4		5 points
5		5 points
6		5 points
7		5 points
Total:		35 points

1a. Show that the alternating group $\mathbf{A}_6$ does not have a subgroup of index 3. (You can assume that $\mathbf{A}_6$ is simple.)

If $H < \mathbf{A}_6$ has index 3, the action by left translation of $\mathbf{A}_6$ on $\mathbf{A}_6/H$ gives a non-trivial homomorphism $\mathbf{A}_6 \to \mathbf{S}_3$. Such a homomorphism must have trivial kernel because of the simplicity of $\mathbf{A}_6$; in other words, the homomorphism is injective. This is ridiculous because the target group has order 6, whereas the source has order 360.

b. Prove that there is no simple group of order 120. [Assume that G is such a group and consider the 5-Sylow subgroups of G.]

Let G be such a group. The number of 5-Sylows of G divides 24 and is 1 mod 5; it can only be 1 or 6. If it's 1, the unique 5-Sylow is normal, which is impossible because G is simple. Therefore there are six 5-Sylow subgroups.

The action of G by conjugation on the set of 5-Sylows of G defines a homomorphism $G \to \mathbf{S}_6$; as in part (a), this homomorphism must be an embedding. The image of G in $\mathbf{S}_6$ must lie in $\mathbf{A}_6$; otherwise the intersection of G with $\mathbf{A}_6$ inside $\mathbf{S}_6$ would be an index-2 subgroup of G. Hence G is an index-3 sugroup of $\mathbf{A}_6$; this is impossible by part (a).

2a. If A is a finite abelian group (written additively), let

$$S_A = \sum_{a \in A} a$$

be the sum of all elements in A. Show that $2 \cdot S_A = 0$.

As a runs over A, so does $-a$. Thus

$$2 \cdot S_A = \sum_{a \in A} a + \sum_{a \in A} (-a) = \sum_{a \in A} (a + (-a)) = \sum_{a \in A} 0 = 0.$$

b. Prove that S_A is non-zero if and only if A has exactly one element of order 2.

In the sum defining S_A, we can pair up elements a with their negatives $-a$. As long as a and $-a$ are different from each other, they will both occur in the sum and cancel each other out. Thus S_A is the sum of those a in A such that $a = -a$. The as like this are the ones for which $2a = 0$. In other words, S_A is the sum of all elements of order 1 or 2 in A. If $A[2] = \{\, a \in A \,|\, 2a = 0 \,\}$, then $S_A = S_{A[2]}$. Thus we can, and will, assume that A is annihilated by 2; thus A consists of 0 and elements of order 2. We have to prove that S_A is non-zero if and only if A has two elements.

If $A = (0)$, then A has no elements of order 2 and $S_A = 0$. Thus the statement is true in this case. Accordingly, we can and will assume that A is non-zero, so that A has an element t of order 2. We partition A into pairs $\{a, a+t\}$; the number of such pairs is one-half the order of A. The sum of the elements in each pair is $a + (a+t) = 2a + t = t$. As a result, $S_A = n \cdot t$, where n is half the order of A. Thus S_A is non-zero if and only if n is odd; this happens if and only if A has two elements, i.e., exactly when A has a unique element of order 2.

3a. Let K be a field and let n be a positive integer prime to the characteristic of K. (If K has characteristic 0, there is no condition on n.) Let $\zeta \in \bar{K}^*$ be a primitive nth root of 1. Prove that $K(\zeta)$ is a Galois extension of K and that $[K(\zeta) : K]$ divides $\varphi(n)$. (Here φ is the Euler phi function.)

The field $K(\zeta)$ is the splitting field of the polynomial $x^n - 1$ because the roots of this polynomial are the powers of ζ. The polynomial has distinct roots because n is non-zero in K. Thus the splitting field is a separable and normal extension—it's a Galois extension of K.

As we discussed in class (and as is explained in Chapter VI of Lang), the Galois group of the extension $K(\zeta)/K$ is naturally a subgroup of the group of automorphisms of the group of nth roots of unity in $K(\zeta)$. This group of automorphisms is $(\mathbf{Z}/n\mathbf{Z})^*$, which has order $\varphi(n)$.

b. If p is a prime number and t is a positive integer, show that the polynomial

$$\frac{x^{p^t}-1}{x^{p^{t-1}}-1} = x^{(p-1)p^{t-1}} + x^{(p-2)p^{t-1}} + \cdots x^{p^{t-1}} + 1$$

is irreducible over $\mathbf{Q}$.

Let $f(x)$ be the polynomial in question. Certainly $f(x)$ is irreducible if and only if $f(x+1)$ is irreducible. We will establish the irreducibilty of $f(x+1)$ by using Eisenstein's criterion (p. 183 of the book) at the prime p. Note that $f(x+1)$ is a monic polynomial whose constant term is $f(1) = 1+1+\cdots+1 = p$. Thus $f(x+1)$ will satisfy Eisenstein's criterion if it is congruent to $x^{(p-1)p^{t-1}}$ mod p.

Let's work mod p. We have

$$(x+1)^{p^t} - 1 = ((x+1)^{p^{t-1}} - 1)f(x+1).$$

But $(x+1)^{p^t} - 1 = ((x+1)-1)^{p^t} = x^{p^t}$ in characteristic p. Similarly, $(x+1)^{p^{t-1}} - 1 = x^{p^{t-1}}$ in characteristic p. Thus $f(x+1)$ is $x^{p^t}/x^{p^{t-1}} = x^{p^{t-1}(p-1)}$, as required.

4. A *prime field* is a field that is either $\mathbf{Q}$ or one of the fields $\mathbf{Z}/p\mathbf{Z}$ with p a prime number.

Let K and L be prime fields. Show that $K \otimes_{\mathbf{Z}} L$ is non-zero if and only if K and L are the same field.

If $K = L$, there is a non-zero bilinear map $K \times K \to K$, namely $(x, y) \mapsto xy$. This map corresponds to a non-zero homomorphism $K \otimes K \to K$; accordingly, the tensor product is non-zero.

If K and L are different, then one of them is $\mathbf{Z}/p\mathbf{Z}$ with p prime and the other is either $\mathbf{Z}/\ell\mathbf{Z}$ with ℓ prime different from p or is the field $\mathbf{Q}$. We know that $\mathbf{Z}/p\mathbf{Z} \otimes \mathbf{Z}/\ell\mathbf{Z}$ is zero because it is killed both by multiplication by p and by ℓ (and hence by multiplication by 1). How about $\mathbf{Z}/p\mathbf{Z} \otimes \mathbf{Q}$? Well, each tensor $a \otimes b$ may be rewritten

$$a \otimes \left(p \cdot \frac{b}{p}\right) = pa \otimes \frac{b}{p} = 0 \otimes \frac{b}{p} = 0.$$

Since $\mathbf{Z}/p\mathbf{Z} \otimes \mathbf{Q}$ is generated by such pure tensors, it is 0. (We could also argue in terms of bilinear maps.)

5. Let A be a Dedekind ring. We know from homework that A is Noetherian; that every non-zero ideal of A is a product of non-zero prime ideals of A; that every non-zero prime ideal of A is maximal.

Suppose that the Dedekind ring A is a unique factorization domain. Show that A is a principal ideal domain:

a. Let $\mathfrak{p}$ be a non-zero prime ideal of A. Show that $\mathfrak{p}$ contains an irreducible element x of A.

Since $\mathfrak{p}$ is non-zero, it contains a non-zero element a of A. Since A is a UFD, we can write a as a product of irreducible elements, say $a = x_1 \cdots x_t$. Because $\mathfrak{p}$ is a prime ideal, one of the x_i must lie in $\mathfrak{p}$.

b. With x as in (a), show that $\mathfrak{p} = (x)$.

In a UFD, the ideal generated by an irreducible element is a prime ideal. (In other words, if an irreducible element π occurs in the factorization of ab, it must appear in the factorization of a or of b.) Thus (x) is prime; hence it is maximal, by the remarks made at the beginning of the problem. Since we have $(x) \subseteq \mathfrak{p}$, the two ideals are equal.

c. Show that every non-zero ideal of A is principal.

Every non-zero ideal of A is a product of prime ideals (as mentioned at the beginning of the problem). A product of principal ideals is principal.

6. Suppose that $f(x)$ is a monic polynomial over a field K with the following unlikely-sounding property: the roots of $f(x)$ in an algebraic closure $\bar{K}$ of K are distinct and form a subfield of $\bar{K}$.

a. Show that the characteristic of K is a prime number p.

A field and its subfields all have the same characteristic. The subfield of $\bar{K}$ formed by the roots of f has only a finite number of elements because a polynomial has only a finite number of roots. Thus this subfield must be of characteristic p for some prime number p. (Fields of characteristic 0 contain $\mathbf{Q}$ and are thus infinite!) It follows that $\bar{K}$ and K have characteristic p as well.

b. Show that $f(x) = x^{p^n} - x$ for some integer $n \geq 1$.

Say that L is the field formed by the roots of $f(x)$. Then L is finite, so it's of order p^n for some $n \geq 1$. As George explained one day when I was traveling, the product $\prod_{\alpha \in L}(x - \alpha)$ is then $x^{p^n} - x$. However, $f(x)$ is also this product: Any monic polynomial factors over $\bar{K}$ as the product of linear factors $x - r$ as r runs over the roots of the polynomial (counted with multiplicity). For $f(x)$, the multiplicites are all 1, by hypothesis. Because the product is both $f(x)$ and $x^{p^n} - x$, these two polynomials are equal.

Note: When the exam was printed, the hypothesis that the roots of $f(x)$ are distinct was omitted. It will be added when the exam is distributed.

Note: This is problem #13 in page 254 of the textbook.

7. Let A be a finite abelian group and let B be a subgroup of A such that the groups B and A/B have relative prime orders. Consider the exact sequence

$$0 \to B \to A \to A/B \to 0,$$

where the second map is the inclusion of B into A and the third map is the quotient map $a \mapsto a + B$. Show that this sequence is *split*.

Note that it is *not* enough to show that A is isomorphic abstractly to the direct sum $B \oplus (A/B)$. See `http://math.stackexchange.com/questions/131881/group-extensions/131895#131895` for a discussion of this point.

Let π be the quotient map. The aim is to find a homomorphism $\sigma : A/B \to A$ such that $\pi \circ \sigma$ is the identity map id on A/B.

By Euclid, we can find an integer $n \geq 1$ that is divisible by the order of B and congruent to 1 mod the order of A/B. The executive summary of what happens now is as follows: we define

$$\sigma(a + B) := n \cdot a \in A;$$

this map is a well-defined homomorphism whose composition with π is the identity because $n = 1$ on A/B.

A more leisurely approach to the situation begins by defining $f : A \to A$ to be the map "multiplication by n." Then the restriction of f to B is 0, while the map induced by f on A/B is the identity. We have a commutative digram of the shape:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B & \longrightarrow & A & \xrightarrow{\pi} & A/B & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle 0} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 0 & \longrightarrow & B & \longrightarrow & A & \xrightarrow{\pi} & A/B & \longrightarrow & 0. \end{array}$$

Because f vanishes on B, it factors through π; this means that there is a homomorphism $\sigma : A/B \to A$ so that $f = \sigma \circ \pi$.

I claim that σ is a splitting of π, meaning that $\pi \circ \sigma = \mathrm{id}$ on A/B. The two sides are equal after right composition with π:

$$(\pi \circ \sigma) \circ \pi = \pi \circ (\sigma \circ \pi) = \pi \circ f = \mathrm{id} \circ \pi.$$

Since π is surjective, the two sides are equal before the composition; this is what we need for a splitting.