FINAL EXAM SOLUTIONS–MATH 505A

1. Let L be a Galois extension of a field K of degree 4. What is the largest possible number of fields there could be strictly between K and L? What is the smallest possible number of such fields? Give examples showing that the bounds you claim are attained.

Such fields are in bijection to the proper nontrivial subgroups of the Galois group G of L over K, which is either cyclic of order 4 or the product of two cyclic groups of order 2. In the first case, there is just one proper subgroup and accordingly only one such field (example: $K = \mathbb{Q}, L = \mathbb{Q}[e^{2\pi i/5}]$). In the second case, there are three such subgroups and accordingly three such fields (example: $K = \mathbb{Q}, L = \mathbb{Q}[\sqrt{3}, \sqrt{5}]$). 2. Let $\omega = e^{2\pi i/7}$ be a primitive 7th root of 1 in $\mathbb{C}$ and let K be the cyclotomic field $\mathbb{Q}[\omega]$. Find values of the exponents a, b, c such that $\alpha = \omega^a + \omega^b + \omega^c$ generates a quadratic extension L of $\mathbb{Q}$ inside K, by identifying the Galois group of K over $\mathbb{Q}$ explicitly and deciding to which subgroup of this group L should correspond.

3. By using a formula in class for the second cohomology group $H^2(\mathbb{Z}_n, A)$ of the cyclic group $\mathbb{Z}_n$ with coefficients in a module A, together with facts about finite fields, show that the only finite division algebras over the field $F = F_p$ with a prime number p of elements are finite extensions of F (Wedderburn's Theorem).

Given such a division algebra D, results in class show that D has a maximal subfield $K = F_{p^n}$ which is a finite (necessarily Galois) extension of F_p of degree n. Isomorphism classes of such algebras with maximal subfield K are then parametrized by elements of $H^2(\mathbb{Z}_n, K^*)$. By the formula for the cohomology groups of a finite cyclic group, this latter group is isomorphic to the quotient $F_p^*/N(K^*)$ of the group of nonzero elements in F_p modulo the subgroup of norms of elements in K^*. by Hilbert's Theorem 90, an element of K^* has norm 1 if and only if it is the $(p-1)$st power of another element in K^* (since the Galois group of K over F_p is generated by the Frobenius automorphisms sending any element to its pth power). Since there are $(p^n - 1)/(p-1)$ distinct $(p-1)$st powers in K^*, there are exactly $p - 1$ distinct norms of elements, these norms filling out F_p^*. Thus the H^2 group is trivial and the only central simple algebras over F_p are matrix rings over it. The only division rings finite over F_p are then its finite extension fields.

4. Let $R = \mathbb{Z}[\sqrt{-3}]$ be the subring of $\mathbb{C}$ generated by $\mathbb{Z}$ and $\sqrt{-3}$. Enlarge the the principal ideal (2) of R to a prime ideal P and show that (2) lies strictly between P^2 and P. Deduce that R is *not* a Dedekind domain.

The ideal (2) may be enlarged to $P = (2, 1 + \sqrt{-3})$, which is prime since the quotient of R by this ideal has order two (it is $\mathbb{Z}_2$ with $\sqrt{-3}$ first adjoined and then identified with 1). Taking product of generators, we see that $P^2 \subset (2)$. The containment is proper because P^2, being generated by $2^2, 2(1 + \sqrt{-3}$, and $(1 + \sqrt{-3})^2 = -2 + 2\sqrt{-3}$, consists solely of elements whose norms are multiples of 8. Hence (2) lies strictly between P^2 and P, as claimed, whence the only prime ideal containing it is P and it is not a product of prime ideals. Thus R cannot be a Dedekind domain (or just observe that it is not integrally closed, violating the definition of Dedekind domain).

5. Give a necessary and sufficient condition for a Dedekind domain R to admit a finitely generated nonfree projective module.

The condition is that the class group of R should not be trivial, or equivalently that R should not be a PID.

6. Give an example of a finite non-Galois extension L of a field K such that there are more fields between K and L than subgroups of the automorphism group G of L over K. Also give an example of an *infinite Galois* extension L' of a field K' such that there are more subgroups of the Galois group G' of L' over K' than fields between K' and L'.

Probably the easiest example in the first case is $K = \mathbb{Q}, L = \mathbb{Q}[2^{1/3}]$. Here the automorphism group is trivial, but there are two fields between K and L (namely K and L themselves), so there are more fields than subgroups. In the second case, it was shown in class that if $K = \mathbb{Q}$ and L is obtained from K by adjoining the square root $\sqrt{p}$ of every prime p, then the Galois group of L is an uncountable direct sum of copies of $\mathbb{Z}_2$. It has more subgroups than there are *subsets* of L, so certainly more subgroups than intermediate fields.

7. By looking at quotients of polynomial rings in infinitely many variables over a field, give an example of a non-Noetherian, non-Artinian ring R such that every prime ideal of R is maximal.

Let k be a field and take the quotient $R = k[x_1, x_2, \ldots]/(x_1^2, x_2^2, \ldots)$. Then R has only one prime ideal, namely $(x_1, x_2, \ldots)$, which is maximal; but R is neither Noetherian nor Artinian (its prime ideal is not finitely generated).

8. Classify the finite-dimensional semisimple algebras over $\mathbb{C}$, the field of complex numbers.

These are just the finite direct sums of matrix rings over $\mathbb{C}$.