1 Math 511b - Test 1 Review

1.1 Fields:

1. Let $K = \mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right)$. Show that K is a Galois extension of $\mathbb{Q}$. What is the Galois group of K over $\mathbb{Q}$?

2. The field $F = \mathbb{Q}\left(\sqrt{2}\right) \vee \mathbb{Q}\left(\sqrt[3]{2}\right)$ is a simple extension of $\mathbb{Q}$. Find a particular primitive element that shows that F is a simple radical extension.

3. If $K \leq \mathbb{C}$ and K is algebraic over $\mathbb{Q}$ show that π is transcendental over K.

4. Suppose $F_0 = \mathbb{F}_4$, the field with 4 elements. Set $F = F_0(t)$, the field of rational functions in the indeterminate t, and say $K = F(a)$, with $a^3 = t$.

   (a) Show that K is separable and normal over F, hence Galois over F.

   (b) Determine the Galois group $G(K : F)$.

5. Suppose F is a finite field of characteristic p.

   (a) Show that every $a \in F$ has a unique p^{th} root in F.

   (b) Show that every $f(x) \in F[x]$ is separable (it is sufficient to assume that $f(x)$ is irreducible).

6. Set $S = \left\{\sqrt{p} : p \in \mathbb{N}\right\}$ and $K = \mathbb{Q}(S) \subseteq \mathbb{R}$. Show that $\sqrt[3]{17} \notin K$.

7. True or false: If K is a Galois extension of F and L is a Galois extension of K, then L is a Galois extension of F.

8. Determine with reasons the number of elements of multiplicative order 9 in the multiplicative group $\mathbb{F}_{64}^*$ of the field with 64 elements.

9. Write C_2 for a cyclic group of order 2. Give an example of a field extension K of $\mathbb{Q}$, $K \subseteq \mathbb{C}$ and Galois over $\mathbb{Q}$ with $Gal(K : \mathbb{Q}) \cong C_2 \times C_2 \times C_2$.

10. Suppose K is a Galois extension of F, and that $Gal(K : F) \cong D_4$, the dihedral group of order 8. Describe as completely as you can the set of intermediate fields L, $F \subset L \subset K$; how many are there, what are the degrees $[L : F]$, which of them are Galois over F?

11. If $z = a + bi \in \mathbb{C}$, calculate $Tr_{\mathbb{C}/\mathbb{R}}(z)$ and $N_{\mathbb{C}/\mathbb{R}}(z)$.

12. Set $F = \mathbb{Q}\left(\sqrt{1+\sqrt{7}}\right)$. Show that F is not Galois over $\mathbb{Q}$. Find explicitly the Galois closure K of F over $\mathbb{Q}$ and determine $Gal(K : \mathbb{Q})$.

13. Determine the Galois group over $\mathbb{Q}$ of $f(x) = x^4 + 5x + 5$.

14. If $f(x) = x^5 + 3x^3 - 3x^2 - 9 \in \mathbb{Q}[x]$, find a splitting field $K \subseteq \mathbb{C}$ and determine its Galois group.

15. Suppose that $f(x) \in \mathbb{Q}[x]$, $g(x) = f\left(x^2\right)$, $K \subset \mathbb{C}$ is a splitting field for $g(x)$ and $[K : \mathbb{Q}]$ is odd. Show that $f(x)$ and $g(x)$ have the same Galois group.

16. Let $K = \mathbb{F}_{81}$, the field with 81 elements with prime field $\mathbb{F}_3$. Determine with reasons the cardinalities of the following two subsets of K.

    (a) $S = \{a \in K : F(a) = L\}$, generators for K as a field extension of F.

    (b) $T = \{a \in K : (a) = K^* = K \setminus \{0\}\}$, generators for the (multiplicative) group K^*.

17. Suppose that $f(x) \in \mathbb{Q}[x]$ is irreducible of degree 4. Show that the Galois group of $f(x)$ cannot be the quaternion group Q of order 8.

1.2 Modules:

1. If F is a field, let R be the ring
$$R = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in F \right\}.$$
Define R-modules
$$M = \left\{ \begin{bmatrix} a \\ 0 \end{bmatrix} : a \in F \right\} \text{ and } N = \left\{ \begin{bmatrix} 0 \\ b \end{bmatrix} : b \in F \right\}.$$
Show that M and N are not isomorphic as R-modules.

2. True or false:

    (a) If M and N are free modules, then so is $M \oplus N$.

    (b) $\mathbb{Q} \oplus \mathbb{Q}$ is a finitely generated $\mathbb{Z}$-module.

    (c) $\mathbb{R} \oplus \mathbb{R}$ is a finitely generated $\mathbb{Q}$-module.

    (d) $\mathbb{C} \oplus \mathbb{C}$ is a finitely generated $\mathbb{R}$-module.

3. Prove or give a counterexample: If R is an integral domain, then $Tor(M) = \{m \in M : \exists r \neq 0 \in R, rm = 0\}$ is a submodule of M.

4. Let M, N be simple R-modules. Prove that any module homomorphism $f : M \to N$ is either an isomorphism or the zero map.

5. If M is a cyclic unitary R-module show that M is R-isomorphic with R/I for some left ideal of R.

6. Suppose that R is a ring with 1, L is a unitary (left) R-module, M and N are submodules of L, and both $M + N$ and $M \cap N$ are finitely generated. Show that M and N are finitely generated.

7. Let T be the $\mathbb{Z}[i]$ module homomorphism from $\mathbb{Z}[i]^2$ to $\mathbb{Z}[i]^2$ defined by the matrix $\begin{pmatrix} 2i & 4i+2 \\ 2i-2 & i \end{pmatrix}$. Determine whether T is one-to-one and whether T is onto.

8. Let R be a PID, let M be a free R-module of finite rank and let f be an R-endomorphism of M. Show that f is injective if and only if $M/\operatorname{Im}(f)$ is an R-torsion submodule.

9. Let R be a nonzero commutative ring with 1. Show that if every submodule of a free R-module is free, then R is a PID.

10. True or false

    (a) Let R be an ID with 1. Then finitely generated torsion-free R-modules are free.

    (b) Let R be a PID. Then torsion-free R-modules are free.

    (c) Let R be an ID with 1. Let F be the field of fractions of R, with V a vector space over F. We may consider V to be an R-module, since R is a subring of F. Then vectors $v_1, ..., v_n \in V$ are linearly independent if and only if they are linearly dependent over R.

    (d) Let R be a commutative ring with an identity element and let M be an R-module. Then M is a finite set if and only if it is finitely generated and every element of M is a torsion element.

11. Let R be a ring and suppose that M_1, M_2, and M_3 are three left R-modules. Let $f : M_1 \to M_2$ be a homomorphism.

    (a) Show that f induces a homomorphism
    $$g : \operatorname{Hom}_R(M_2, M_3) \to \operatorname{Hom}_R(M_1, M_3)$$

    (b) Show that if f is surjective, then g is injective.

    (c) If f is injective, is g surjective? Give a proof or counterexample.

12. Let M be the $\mathbb{Z}$-module $\mathbb{Z}\oplus(\mathbb{Z}/3\mathbb{Z})$. Give a precise and explicit description of $\operatorname{End}_{\mathbb{Z}}(M)$.

13. Let $T : V \to V$ is a linear transformation and regard V as a $\mathbb{C}[x]$-module via T (that is define $x(v) = T(v)$). Suppose that the minimal polynomial of T has degree equal to the dimension of V. Show that V is a cyclic $\mathbb{C}[x]$-module.

14. Let $f : \mathbb{Z}^2 \longrightarrow \mathbb{Z}/3\mathbb{Z}$ be the homomorphism $f(x, y) = x + y \pmod 3$.

    (a) Find a $\mathbb{Z}$-module basis for $K = \ker(f)$.

    (b) Does there exist a $\mathbb{Z}$-module homomorphism $g : \mathbb{Z}^2 \to K$ such that the composition $K \to \mathbb{Z}^2 \to K$ of g with the inclusion map is the identity? Why or why not?