ALGEBRA PRELIM REVIEW

Linear Algebra

(1) Let V be an n-dimensional K-vector space, and let $U \subset V$ be a subspace of positive dimension $r < n$. Let $\varphi : V \to V$ be a K-linear map with $\varphi(U) \subset U$. Argue that:

(a) There is an ordered basis B of V such that the coordinate matrix $A_\varphi^{B,B}$ has the form
$$A_\varphi^{B,B} = \begin{bmatrix} M & N \\ 0 & P \end{bmatrix}$$
where $M \in K^{r \times r}$ and $P \in K(n-r) \times (n-r)$.

(b) If $im(\varphi) \subset U$, then one can choose B such that $P = 0$.

(2) Consider the map $\varphi : \mathbb{Q}^{2\times 2} \to \mathbb{Q}^{2\times 2}$ given by $A \mapsto AM - MA$, where
$$M = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in \mathbb{Q}^{2\times 2}$$
.

(a) Show that φ is a $\mathbb{Q}$-linear map.

(b) Find a basis for $ker(\varphi)$ and determine its dimension.

(3) Consider a matrix $A \in K^{n\times n}$, where K is a field. Show:

(a) If $rk(A) < n$, then there is a matrix $0 \neq B \in K^{n\times n}$ such that $A \cdot B = 0$

(b) If $A^k = 0$ for some $k \in \mathbb{N}$, then A is not invertible.

(4) Let V be a 4-dimensional vector space, and let $U_1, U_2 \subset V$ be two 3-dimensional subspaces of V.

(a) Determine the possible values of $m = dim(U_1 \cap U_2)$.

(b) For each value of m in (a), give an example of subspaces $U_1, U_2 \subset V = \mathbb{Q}^4$ whose intersection has dimension m.

(5) Let $U \subset K^n$ be a subspace, and consider the set
$$V := \{\varphi \in Hom(K^n, K^m) \mid U \subset ker(\varphi)\}$$

Prove:

(a) V is a K-vector space.

(b) $dim(V) = m(n - dim(U))$.

(6) (6/16) In the real vector space of continuous real-valued functions on $\mathbb{R}$, consider the functions $p_i, i = 0, 1, 2$ and exp defined by $p_i(x) = x^i$ and $exp(x) = e^x$ for $x \in \mathbb{R}$. Set $V := span_{\mathbb{R}}\{p_0, p_1, p_2, exp\}$ and consider the endomorphism $\sigma : V \to V$ defined by $(\sigma f)(x) := f(x-1)$ for $x \in \mathbb{R}$.

(a) Give the matrix representation of σ with respect to the basis $\{p_0, p_1, p_2, exp\}$.

(b) Determine all the eigenvalues and find the bases of all eigenspaces of σ.

(c) Is σ diagonalizable?
(d) Determine the minimal polynomial of σ.

(7) Let A, B, C be square matrices over a field K such that $A = \begin{bmatrix} B & 0 \\ 0 & C \end{bmatrix}$. Argue that their minimal polynomials satisfy $\mu_A = lcm(\mu_B, \mu_C)$, where lcm denotes the least common multiple.

(8) (6/14) Consider a linear transformation T on a vector space V of dimension 4 over $\mathbb{R}$. On a basis e_1, e_2, e_3, e_4 of V, the transformation is defined by $T(e_1) = e_2$, $T(e_2) = e_1$, $T(e_3) = 2e_3 + e_4$, and $T(e_4) = e_3 - 2e_4$.
(a) Construct the matrix A of the transformation with respect to the given basis.
(b) Determine the characteristic polynomial, eigenvalues, and eigenspaces of A.
(c) Determine the kernel and image of the transformation defined by the matrix $A^2 - I$ on $\mathbb{R}^4$.
(d) Is A diagonalizable? Would you answer differently if $\mathbb{R}$ was replaced by $\mathbb{Q}$?

(9) (1/09) Let $n \in \mathbb{N}$ and F be a field. Suppose that $T : F \to F^n$ is a linear transformation. Show that T is injective if and only if T is not the zero map.

(10) (6/11) Let $A \in M_{n\times n}(\mathbb{C})$ be a Hermitian matrix. Prove or disprove (with a counterexample) the following statements:
(a) $det(A) \in \mathbb{R}$.
(b) $|det(A)| = 1$.
(c) If A has exactly one eigenvalue, then A is a real matrix.
(d) If $v = (v_1, \ldots, v_n)^T$ is an eigenvector of A, then $\overline{v} = (\overline{v_1}, \ldots, \overline{v_n})^T$ is also an eigenvector of A (where $\overline{v_i}$ denotes the complex conjugate of v_i).

Group Theory

(1) (N53) Let G be an abelian group and let $a, b \in G$ be elements of finite order m and n, respectively.
  (a) Show that $ord(ab) \leq e$, where e is the positive least common multiple of m and n.
  (b) Decide whether equality is always true in (a).
  (c) If m and n are relatively prime, argue that $ord(ab) = mn$.

(2) (N67) Let H be a subgroup of a group G, and denote by $P(G)$ the set of all subsets of G. Show:
  (a) G acts on $P(G)$ by conjugation, i.e., $G \times P(G) \to P(G)$ is given by $(g, M) \mapsto gMg^{-1}$. (For every non-empty subset $M \subset G$, the stabilizer of M with respect to this action is the *normalizer* $N_G(M)$ of M in G).
  (b) $H \lhd N_G(H) < G$.
  (c) $H \lhd G$ if and only if $N_G(H) = G$.
  (d) If G is finite, then $[G : N_G(H)]$ is the number of subgroups of G that are conjugates of H.

(3) (N68, 6/16, 6/11) Prove that a group G is abelian if $G/Z(G)$ is a cyclic group.

(4) (DF4.2.8) Prove that if H has finite index n, then there is a normal subgroup K of G with $K \leq H$ and $|G : K| \leq n!$.

(5) (DF4.2.14) Let G be a finite group of composite order n with the property that G has a subgroup of order k for each positive integer k dividing n. Prove that G is not simple.

(6) (DF4.3.34) Prove that if p is a prime and P is a subgroup of S_p of order p, then $|N_{S_p}(P)| = p(p-1)$. [Hint: Argue that every conjugate of P contains exactly $p-1$ p-cycles and use the formula for the number of p-cycles to compute the index of N_{S_p} in S_p].

(7) (DF4.4.2) Prove that if G is an abelian group of order pq, where p and q are distinct primes, then G is cyclic. [Hint: Use Cauchy's theorem to produce elements of order p and q and consider the order of their product].

(8) (DF4.4.13) Let G be a group of order 203. Prove that if H is a normal subgroup of order 7 in G then $H \leq Z(G)$. Deduce that G is abelian in this case.

(9) (DF4.5.15) Prove that a group of order 351 has a normal Sylow p-subgroup for some prime p dividing its order.

(10) (DF4.5.35) Let $P \in Syl_p(G)$ and let $H \leq G$. Prove that $gPg_{-1} \cap H$ is a Sylow p-subgroup of H for some $g \in G$. Give an explicit example showing that $hPh^{-1} \cap H$ is not necessarily a Sylow p-subgroup of H for any $h \in H$ (in particular, we cannot

always take $g = 1$ in the first part of this problem, as we could when H was normal in G.

Field and Galois Theory

Note: We denote by $G(E,K)$ the Galois group of E/K, that is, the subgroup of $Aut(E)$ consisting of K-homomorphisms.

(1) (N45) Let E/K be a field extension of degree 2 and assume that the characteristic of K is not 2. Show that:
 (a) E/K is a simple field extension.
 (b) There are exactly two K-automorphisms of E.
 (c) If $f \in K[x]$ is irreducible and has a root in E, then f splits over E.

(2) (N60) Let K be a prime field of finite order p and let $f \in K[x]$ be an irreducible polynomial. For every positive integer n, show that $deg(f) \mid n$ iff $f \mid (x^{p^n} - x)$.

(3) (N55) Let E/K be a Galois field extension and let L_1, L_2 be subfields of E that contain K. Prove:
 (a) $G(E, L_1L_2) = G(E, L_1) \cap G(E, L_2)$
 (b) $G(E, L_1 \cap L_2)$ is the subgroup of $G(E,K)$ that is generated by $G(E, L_1)$ and $G(E, L_2)$.

(4) (N57) Prove that $[\mathbb{Q}(\sqrt(2), \sqrt(3), \sqrt(5)) : \mathbb{Q}] = 8$.

(5) (N58) Let E/K be any field extension where E is finite. Show:
 (a) E/K is a Galois extension.
 (b) The Galois group $G(E,K)$ is cyclic. Specify a map that generates the group.

(6) (N73) Let E be a splitting field of an irreducible and separable polynomial $f \in K[x]$ over a field K. Denote by $\alpha_1, \ldots, \alpha_n \in E$ the roots of f. Assume that the Galois group $G(E,K)$ is abelian. Show that $E = K(\alpha_i)$ for each $i = 1, \ldots, n$, and so $[E : K] = deg(f)$.

(7) (N87) Determine the Galois groups of the polynomials $f := x^3 + 6x^2 + 11x + 7$ and $g := x^3 + 3x^2 - 1$ in $\mathbb{Q}[x]$. Besides giving the isomorphism type of the group, describe the automorphisms explicitly.

(8) (6/14) Let $f(x) = (x^3 - 5)(x^5 - 7) \in \mathbb{Q}[x]$, and let K be a splitting field of $f(x)$ over $\mathbb{Q}$. Let $n = [K : \mathbb{Q}]$.
 (a) Argue that n is divisible by 15.
 (b) Show that K must contain a primitive 15th root of unity over $\mathbb{Q}$ which satisfies a monic polynomial of degree 8.
 (c) Deduce that $n = 120$.

(9) (1/13) Let $n \geq 3$ and let ζ be a primitive nth root of unity over $\mathbb{Q}$. Recall that $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$, where φ is the Euler φ-function. Prove that $\alpha := \zeta + \zeta^{-1}$ is algebraic over $\mathbb{Q}$ of degree $\varphi(n)/2$. [Hint: It will be useful to note that $\alpha \in \mathbb{R}$. If you want to use this fact then you also have to prove it].

(10) (5/15) Consider the field extension $\mathbb{F}_{5^4}|\mathbb{F}_5$.

(a) Determine the number of elements $a \in \mathbb{F}_{5^4}$ satisfying $\mathbb{F}_{5^4} = \mathbb{F}_5(a)$.

(b) Determine the number of irreducible polynomials of degree 4 in $\mathbb{F}_5[x]$.

Ring Theory

(1) (N18) Find all ring homomorphisms $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$.

(2) (N20) Convince yourself that the set $R := \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ is differentiable}\}$ is a commutative ring with the usual sum and product of functions. Prove:
  (a) The set $I := \{f \in R \mid f(5) = f'(5) = 0\}$ is an ideal of R.
  (b) $\mathbb{R}[x]/(x^2) = \{(a + bx) mod(x^2) \mid a, b \in \mathbb{R}\}$.
  (c) The rings R/I and $\mathbb{R}[x]/(x^2)$ are isomorphic.

(3) (N21) Let I and J be ideals of a ring R and let $\pi : R \to R/I$ be the canonical epimorphism. Show:
  (a) $\pi(J)$ is an ideal in R/I (it is denoted $(J + I)/I$).
  (b) π induces an inclusion-preserving bijection

$$\{J \mid J \text{ is an ideal of } R \text{ such that } I \subset J\} \to \{\text{ideals of } R/I\}.$$

(4) (N25) Let I be an ideal in a ring R, and let $\varphi : R \to S$ be a ring homomorphism. Prove that φ factors through the canonical epimorphism $\pi : R \to R/I$, i.e., there is a ring homomorphism $\psi : R/I \to S$ such that $\varphi = \psi \circ \pi$, if and only if $I \subset ker(\varphi)$.

(5) (N27) Let p be a fixed prime and consider the set

$$R := \{\frac{a}{b} \mid a, b \in \mathbb{Z} \text{ are coprime}, p \nmid b\}.$$

  (a) Show that R is a subring of $\mathbb{Q}$ and not a field.
  (b) Determine the set of units $R^\times$.
  (c) Show that each non-zero ideal of R is principal and of the form (p^e) for some $e \in \mathbb{N}_0$.

(6) (N31) Let I be an ideal of a ring R. If R is a PID, show that every ideal of R/I is principal. Is the converse true?

(7) (N32) Consider the ring $R := \mathbb{Q}[x]/(x - 1)(x + 2)$.
  (a) Determine all ideals of R.
  (b) Find (up to isomorphism) all rings S such that there is a surjective ring homomorphism $R \to S$.

(8) (N38) Let R be a factorial domain with the property that every ideal that is generated by two elements is a principal ideal. Prove the R must be a PID.

(9) (N39,41) Show that the following polynomials are irreducible in the given ring:
  (a) $2x^4 + 200x^3 + 40x^2 + 2000x + 20 \in \mathbb{Q}[x]$
  (b) $(y + 8)^2x^3 - x^2 + (y + 7)(y + 8) - y - 12 \in \mathbb{Q}[x, y]$
  (c) $x^2y + xy^2 - x - y + 1 \in \mathbb{Q}[x, y]$
  (d) $2 + i \in \mathbb{Z}[i]$ (as an element)
  (e) $x^n - 2 - i \in \mathbb{Q}(i)[x]$ for every positive integer n (you may use that the quotient field of $\mathbb{Z}[i]$ is $\mathbb{Q}(i)$).

(10) (5/15) Consider the ring $\mathbb{Z}[i]$ if Gaussian integers and let f be the ring homomorphism

$$f : \mathbb{Z} \to \mathbb{Z}[i]/(3+2i),\ c \mapsto c + (3+2i).$$

Show the following:

(a) f is surjective.
(b) $ker(f) = 13\mathbb{Z}$.
(c) $|\mathbb{Z}[i]/(3+2i)| = 13$.

(11) (DF 7.6.3, 6/16) Let R and S be commutative rings with identity. Prove that every ideal of $R \times S$ is of the form $I \times J$ where I and J are ideals of R and S, respectively.

(12) (DF 7.6.4) Prove that if R and S are nonzero rings, then $R \times S$ is never a field.