Additional Problems

1. Let A be a commutative ring and let

$$0 \to M \overset{\alpha}{\to} N \overset{\beta}{\to} P \to 0$$

be a short exact sequence of A-modules. Let Q be an A-module.
i) Show that the naturally induced sequence

$$0 \to Hom(P,Q) \overset{\circ\beta}{\to} Hom(N,Q) \overset{\circ\alpha}{\to} Hom(M,Q)$$

is exact, but that

$$Hom(N,Q) \overset{\circ\alpha}{\to} Hom(M,Q)$$

is not necessarily surjective.
ii) Show that the naturally induced sequence

$$Q \otimes M \overset{id\otimes\alpha}{\to} Q \otimes N \overset{id\otimes\beta}{\to} Q \otimes P \to 0$$

is exact.

2. Let I and J be ideals in a commutative ring A. Give a simple description of $(A/I) \otimes (A/J)$.

3. Let M and N be cyclic modules over a principal ideal domain R. The module $tor_R(M,N)$ is defined as follows. (This is a special case of a more general construction.) Take an exact sequence

$$0 \to R \to R \to M \to 0$$

Then $tor_R(M,N)$ is defined by the exactness of the sequence

$$0 \to tor_R(M,N) \to N \otimes R \to N \otimes R \to N \otimes M \to 0$$

(Note: $N \otimes R = N$.)
i) Describe $tor_R(M,N)$ in simple terms.
ii) Show that $tor_R(M,N) \simeq tor_R(N,M)$.

4. Let k be a field and let $S : k^n \to k^n$ and $T : k^m \to k^m$ be k-linear endomorphisms.
i) Find the determinant of $S \otimes T : k^n \otimes k^m \to k^n \otimes k^m$.
ii) Find the trace of $S \otimes T : k^n \otimes k^m \to k^n \otimes k^m$.

MATH 8000 Homework 14, due Monday 12/07/09.

1. Read the definition of composite field on page 528. Let N/F and E/F be algebraic field extensions, with N normal. Let $\psi : E \to C$ be an algebraic closure. Let $\phi : N \to C$ be a homomorphism such that $\psi|_F = \phi|_F$.
i) Show that, up to isomorphism, the composite field $\phi(N)\psi(E)$ is independent of the choice of C, ψ and ϕ. We call it the composite of N and E, and denote it NE.
ii) Show that the intersection $\phi(N) \cap \psi(E)$ is also independent of the choices. We denote it $N \cap E$.

2. Read proposition 14.4.19. Let N/F and E/F be finite extensions, with N Galois. Assume that $N \cap E = F$. Show that

$$Gal(NE/F) \simeq Gal(NE/N) \rtimes Gal(NE/E)$$

3. Let n be a nonnegative integer. Let $0 \neq a \in \mathbb{Q}$ and let $\theta \in \mathbb{C}$ such that $\theta^n = a$. Let $\omega \in \mathbb{C}$ be a primitive n^{th} root of unity. Assume $\mathbb{Q}(\omega) \cap \mathbb{Q}(\theta) = \mathbb{Q}$. Let d be the degree of the minimal polynomial of θ over $\mathbb{Q}$. Prove that $d|n$, and that furthermore, $Gal_{\mathbb{Q}}(x^n - a) = \mathbb{Z}_d \rtimes \mathbb{Z}_n^*$.
($\mathbb{Z}_n^*$ acts on $\mathbb{Z}_d$ as follows. Identify $\mathbb{Z}_n^*$ with $Aut(\mathbb{Z}_n)$. Since there is a unique copy of $\mathbb{Z}_d$ inside $\mathbb{Z}_n$, $Aut(\mathbb{Z}_n)$ acts on it.)

4. Give generators and relations for $Gal_{\mathbb{Q}}(x^8 - 3)$.

5. Give generators and relations for $Gal_{\mathbb{Q}}(x^8 - 9)$.

6. Here is yet another proof of the Cayley-Hamilton theorem.
i) The Cayley-Hamilton theorem for an $n \times n$ matrix is a collection of n^2 polynomial identities, over $\mathbb{Z}$, in n^2 indeterminates, namely the entries of the matrix. Show therefore that if the Cayley-Hamilton theorem holds for every $n \times n$ matrix over your favorite field of characteristic zero, it holds for every $n \times n$ matrix over an arbitrary commutative ring.
ii) Fix a positive integer n, and let A be an $n \times n$ matrix over $\mathbb{C}$. Give an easy argument that proves the Cayley-Hamilton theorem holds if A has distinct eigenvalues.
iii) Prove that there is a polynomial $p(a_{i,j})$ in the entries of A such that A has distinct eigenvalues if and only if $p(a_{i,j}) \neq 0$. (Hint: See page 610.) Therefore, if f_A is the characteristic polynomial of A, then $p(a_{i,j})f_A(A) = 0$.
iv) Conclude that $f_A(A) = 0$.

DF 14.2: 21,22, 23 14.6: 27

MATH 8000 Homework 13, due Friday 11/20/09.

1. Sept. '92, #5

2. Sept. '93, #3

3. May '95, #4

4. Fall '02, #5

5. Let $\lambda \in \mathbb{C}$, $\lambda^5 = 1$. Let $f(z) \in \mathbb{C}[z]$ and suppose that for all z, $f(\lambda z)^2 - z^5 f(\lambda z) = f(z)^2 - z^5 f(z)$. Show that $f(\lambda z) = f(z)$.

6. Write $t_1^3 + t_2^3 + t_3^3$ as a polynomial in the elementary symmetric polynomials in t_1, t_2, t_3.

DF 14.1: 8 14.2: 6, 13, 14

MATH 8000 Homework 12, due Friday 11/13/09.

1. Let $F \subset L \subset N$ be a tower of fields, such that N is normal over F. Prove that every F-homomorphism $\phi : L \to N$ extends to a homomorphism $\psi : N \to N$. (Hint: Let C/N be an algebraic closure. First show that ϕ extends to a homomorphism $\psi : N \to C$ and then show that $\psi(N) \subset N$.)

2. Let f and g be polynomials over a field F. Prove that there is a field extension E/F in which f and g have a common root if and only if f and g have a common factor in $F[x]$.

3. Find $Fix(Gal(\mathbb{Q}[2^{1/3}]/\mathbb{Q}))$.

4. Let E/F be an algebraic extension, and let $\phi : F \to C$ be a homomorphism from F to an algebraically closed field C. Prove that the cardinality of the set $Hom_\phi(E, C)$ is independent of the choice of ϕ.

5. Let E/F be a field extension, and let $E_{sep} \subset E$ denote the set of elements $\alpha \in E$ such that α is separable over F. Prove that E_{sep} is a field.

6. Let E be the splitting field of separable polynomial $f \in F[x]$. Prove that E/F is separable.

DF 13.4: 1, 2 13.5: 7

MATH 8000 Homework 11, due Monday 11/09/09.
DF 13.1: 1, 5 13.2: 1, 5, 7, 10, 13, 17, 18

MATH 8000 Homework 10, due Wednesday 11/04/09.

1. Let R be a domain. Given an R-module M and a prime $p \in R$, the p-torsion

part of M is the submodule

$$p\text{-Tor}(M) = \{m \in M \mid \exists n \in \mathbb{N}, p^n m = 0\}$$

p-Tor(M) is also called the *p-primary* part of M. Prove that if M is a torsion module over a PID R, then

$$M = \oplus_p p\text{-}Tor(M)$$

2. Let M be a finitely generated torsion module over a PID R. Let $d_1, d_2, ..., d_k$ be the invariant factors obtained from a presentation matrix of M. Here is a proof that the invariant factors depend only on M and not on the presentation. If one factors each d_i into primes, one may apply the Chinese Remainder Theorem to each R/d_i to obtain the decomposition of R/d_i into its p-primary parts, p prime. For a fixed prime p, we then get an invariant factor decomposition of the p-primary part of M by adding the contributions from each R/d_i. One can recover $d_1, ..., d_k$ from all the invariant factor decompositions of the p-primary parts of M as p varies over all the primes in M. So to recover the invariant factors in general, it suffices to consider the case that M itself is p-primary for some p. Thus we may assume

$$M = R/p^{n_1} \oplus R/p^{n_2} \oplus \dots$$

with $n_1 \leq n_2 \dots$. Let F denote the field R/p.
i) Show that for all nonnegative integers k, $p^k M/p^{k+1}M$ is an F-vector space.
ii) Let r_k denote the dimension of the F-vector space $p^k M/p^{k+1}M$. (Notice that these numbers depend only on M and not on the presentation matrix.) Show that $n_1, n_2, \dots$ can be recovered from $r_1, r_2, \dots$. (This should remind you of a problem from homework 8.)

3. Find the invariant factor decomposition and the primary decomposition of the abelian group presented as follows:

$$\begin{aligned} 10a + 270c + 20d &= 0 \\ 15a + 540c + 30d &= 0 \\ 40a + 30b + 60d &= 0 \\ 60a + 60b + 90d &= 0 \end{aligned}$$

4. Find the rational canonical form of the following matrix:

$$\begin{pmatrix} 1 & 0 & -1 & -1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

5. Let A be a square matrix with entries in a principal ideal domain R. Let M_A denote the R-module with presentation matrix A. Prove that M_A is isomorphic to M_{A^t}, where A^t is the transpose of A.

MATH 8000 Homework 9, due Friday 10/23/09.

1. Let R be a commutative ring and let $A_1, ..., A_k$ be pairwise relatively prime ideals in R. Let M be an R-module such that $\Pi_{i=1}^k A_i \subset ann(M)$. Let $M_i \subset M$ denote the submodule annihilated by A_i. Prove that $M \simeq \oplus_{i=1}^k M_i$.

Hint: Let $e_j \in \Pi_{i=1}^k R/A_i$ denote the k-tuple with 1 in position j and zeroes elsewhere. Let $\phi : R \to \Pi_{i=1}^k R/A_i$ be the natural homomorphism. Use the Chinese Remainder Theorem to establish the existence of $\alpha_i \in R$ such that
a) $\phi(\alpha_i) = e_i$
b) $\sum \alpha_i \equiv 1 \text{mod } \Pi_{i=1}^k A_i$
c) $\alpha_i \in \Pi_{j \neq i}^k A_j$
Then for all $m \in M$, let $m_i = \alpha_i m$.

2. Let k be a field. Let $A \in M_n(k)$ be a square matrix such that the characteristic polynomial of A factors into linear factors over k. For each eigenvalue λ of A, define the *generalized eigenspace* to be the subspace

$$M_\lambda = \{v \in k^n \ : \ \exists j \in \mathbb{N} \ (A - \lambda I)^j v = 0\}$$

Use the Cayley-Hamilton theorem together with problem 1 to show that $k^n = \oplus_\lambda M_\lambda$. Thus k^n is the direct sum of the generalized eigenspaces for A. (Hint: Regard k^n as a $k[x]$-module.)
DF 10.1: 8bc, 12 10.2: 6, 13 10.3: 2, 5, 27 10.5: 1bc, 2, 14

MATH 8000 Homework 8, due Friday 10/16/09.

1. ("mod p cancellation law") Let p be a prime number. Prove that if n and j are nonnegative integers, and we set $n = ap + b$ and $j = cp + d$, with $0 \leq b < p$ and $0 \leq d < p$, then

$$\binom{n}{j} \equiv \binom{a}{c}\binom{b}{d} \ mod \ p$$

(Hint: Think about $(1 + x)^n$ mod p.)

2. Let A be a nilpotent matrix over a field. For each positive integer j, let $b(j)$ denote the number of Jordan blocks of size j in the Jordan form of A, and let $n(j)$ denote the nullity of A^j. Establish an explicit formula for the $b(j)$'s in terms of the $n(j)$'s.

3. Let

$$f = z^3 + z^2x^2 + z^2y^3 + z^2y + zyx^5 + x + xz^3 + z^2x^3 + xz^2y^3 + xz^2y + zyx^6 + x^2$$

i) Find the irreducible factors of f as an element of $\mathbb{Z}[x, y, z]$.
ii) Find the irreducible factors of f as an element of $\mathbb{Q}(x, y)[z]$.
suggestion: Write f as a polynomial in z with coefficients in $\mathbb{Z}[x, y]$.
DF 9.2: 7 9.3: 1,4 9.4: 1, 6, 9, 11, 12, 15, 16

MATH 8000 Homework 7, due Friday 10/02/09.

1. Let $S \subset \mathbb{Z}_{18}$ be the set of powers of 2. Then the ring $S^{-1}\mathbb{Z}_{18}$ is a familiar ring. Which one?

2. Show by example that if R is a commutative ring and $S \subset R$ is a multiplicative subset, then the relation on $R \times S$ given by $(r, s) \sim (r', s') \Leftrightarrow rs' - r's = 0$ need not be an equivalence relation.

The next two problems use problem 3 from the last homework.

3. (The Cayley-Hamilton Theorem) Let k be a field and let $A \in M_n(k)$. Let $\xi_A(x)$ denote the characteristic polynomial, $\xi_A(x) = det(xI - A) \in k[x]$.

Theorem (Cayley-Hamilton): $\xi_A(A) = 0$ (You can't prove this by plugging in A for x in the definition!)

Here is one of many proofs: Regard k^n as a $k[x]$-module, by letting a polynomial $p(x)$ act by $p(A)$. The goal then is to prove that $\xi_A(x)$ acts by 0. Do this by verifying the hypotheses of HW 6 problem 3, using the matrix $xI - A$ regarded as an element of $M_n(k[x])$.

4. (Integral closure) Let R be a subring of a commutative ring S and let $s \in S$. Then we say that s is *integral over* R if there is a monic polynomial $p(x) \in R[x]$ such $p(s) = 0$. (For example, $\sqrt{2}$ is integral over $\mathbb{Z}$, while $\frac{1}{\sqrt{2}}$ is not.) The *integral closure* of R in S is the set of elements $s \in S$ integral over R.

Theorem: The integral closure of R in S is a subring.

The proof is as follows: Let s and t be integral over R, and let $R[s, t] \subset S$ be the R-subalgebra generated by s and t. We must show that for all $u \in R[s, t]$, u is integral over R.
i) Show that $R[s, t]$ is a finitely generated R-module.
ii) Let $v_1, ..., v_n \in R[s, t]$ generate $R[s, t]$ as an R-module. Then there is a matrix $(A_{i,j})$ over R such that $uv_j = \sum_i A_{i,j}v_i$ for all j. (Say why.) Use HW 6 problem 3 to prove that u is a root of the polynomial $det(xI - A)$. (This is not quite a corollary of the Cayley-Hamilton theorem, because $v_1, ..., v_n$ need not be a basis.)
iii) Find a monic polynomial in $\mathbb{Z}[x]$ satisfied by $a + b$, given that

$$a^2 - a - 1 = 0$$
$$b^2 - 2b - 1 = 0$$

DF 7.4: 36, 37   7.5: 5,6   8.1: 8   8.2: 8

MATH 8000 Homework 6, due Friday 9/25/09.

1. Let R be a ring, and let M be a free, finitely generated R-module. Prove that $End_R(M)$ is isomorphic to a ring of matrices. (Note that R is not assumed to be commutative.)

2. (Cramer's rule) The solution to this exercise may be found in many texts, but you should know the proof. Let R be a commutative ring, and let $A = (A_{i,j})$ be an $n \times n$ matrix over R. The indexing convention being used here is that if $e_1, ..., e_n$ denotes the standard basis for R^n, then $Ae_j = \sum_i A_{i,j} e_i$. Let $a_1, ..., a_n$ denote the columns of A. The *adjugate* of A, denoted A^{adj}, is the matrix $(B_{i,j})$ defined by

$$B_{i,j} = det(a_1, ..., a_{i-1}, e_j, a_{i+1}, ..., a_n)$$

That is, substitute e_j in place of a_i and take the determinant.
i) Prove that that $BA = det(A)I$.
ii) Write an equivalent definition of A^{adj} using the rows of A, and use it to conclude that $AB = det(A)I$.

3. Here is a useful application of the adjugate. Let R be a commutative ring, and let M be a finitely generated R-module. Then the ring of matrices $M_n(R)$ acts by matrix multiplication on M^n, regarded as column vectors. Let $A \in M_n(R)$ and suppose there exists a set of generators $m_1, ..., m_n$ for M, such that

$$A \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0$$

Prove that $det(A)$ annihilates M.

DF
7.1: 23, 26, 27   7.2: 3, 5, 7   7.3: 29, 33, 34cd   7.4: 33

MATH 8000 Homework 5, due Friday 9/18/09.

1. Let G denote the group of affine linear automorphisms of $\mathbb{R}^n$, i.e, functions of the form $f(x) = Ax + b$, where $A \in Gl_n(\mathbb{R})$ and $x, b \in \mathbb{R}^n$. The group law on G is composition of functions. Prove that $G \simeq \mathbb{R}^n \rtimes_\phi Gl_n(\mathbb{R})$ for an appropriate choice of ϕ.

2. Let H and K be groups. Let $Hom(K, Aut(H))$ be the set of homomorphisms from K to $Aut(H)$. Let $\phi \in Hom(K, Aut(H))$.

i) Find an action of $Aut(H)$ on $Hom(K, Aut(H))$ such that for all $\beta \in Aut(H)$, the function

$$\begin{aligned} \psi : H \times K &\to H \times K \\ \psi(h,k) &= (\beta(h), k) \end{aligned}$$

is an isomorphism

$$\psi : H \rtimes_{\phi} K \to H \rtimes_{\beta * \phi} K$$

ii) Find an action of $Aut(K)$ on $Hom(K, Aut(H))$ such that for all $\alpha \in Aut(K)$, the function

$$\begin{aligned} \psi : H \times K &\to H \times K \\ \psi(h,k) &= (h, \alpha(k)) \end{aligned}$$

is an isomorphism

$$\psi : H \rtimes_{\phi} K \to H \rtimes_{\alpha * \phi} K$$

3. Let $\sigma \in S_n$ for some n. Let k be a field. Consider the linear transformation

$$T_\sigma : k^n \to k^n$$
$$T_\sigma \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_{\sigma^{-1}(1)} \\ x_{\sigma^{-1}(2)} \\ \vdots \\ x_{\sigma^{-1}(n)} \end{pmatrix}$$

i) Let P_σ denote the standard matrix of T_σ. Describe P_σ. (A convincing example will be sufficient proof.) Matrices of the form P_σ for some $\sigma \in S_n$ are called *permutation matrices.*
ii) Prove that the function $S_n \to Gl_n(k)$ sending $\sigma \to P_\sigma$ is a homomorphism.
iii) Prove that $sign(\sigma) = det(P_\sigma)$. (Some authors take this as the definition of the *sign* homomorphism. That would be cheating.)

4. (apropos Spring 04,#9) Let $A \in M_{2\times 2}(\mathbb{R})$ be a 2×2 matrix. Let $v \in \mathbb{C}^2$ be an eigenvector for A, with nonreal eigenvalue λ.
i) Prove that $v, \bar{v}$ form a basis for $\mathbb{C}^2$ and that this basis diagonalizes A.
ii) Prove that $Re(v), Im(v)$ form a basis for $\mathbb{R}^2$.
iii) Letting $\lambda = re^{i\theta}$, find the matrix for the linear transformation defined by A, in the basis $Re(v), Im(v)$.

5. Construct a nonabelian group of order 75.
DF 4.5.19, 4.5.24, 4.5.36, 5.5.2

MATH 8000 Homework 4, due Monday 9/14/09.

1. Let K be a field and let V be a finite-dimensional vector space over K. A *complete flag* over V is a sequence of subspaces

$$\{0\} = W_0 \subset W_1 \subset W_2 \subset \cdots \subset W_n = V$$

such that $dim(W_i) = i$.
i) Let $\mathcal{F}_n(K)$ denote the set of all complete flags over the vector space K^n. Show that $Gl_n(F)$ acts transitively on $\mathcal{F}_n(K)$.
ii) Describe the stabilizer of the *standard flag*, W_i =span$(e_1, \dots, e_i)$, where $e_1, \dots, e_n$ is the standard basis.

2. Let p be a prime integer, and n an integer. Let $H \subset Gl_n(\mathbb{F}_p)$ be the subgroup consisting of matrices with ones on the diagonal and zeroes below the diagonal. Prove that H is a Sylow p-subgroup of $Gl_n(\mathbb{F}_p)$.

3. Find a Sylow 3-subgroup for S_i, $i = 1, ..., 9$. (You may give your answer by providing a set of generators for the group.)

DF 4.2.7b, 4.3.5, 4.3.13, 4.3.17, 4.3.34, 4.4.11

MATH 8000 Homework 3, due Friday 9/04/09.

1. Let G be a group and let $H \subset G$ be a subgroup. Let X denote the set of right H-cosets. Then G acts transitively on X. Therefore, as a G-set, X is isomorphic to some left coset space. Which one, and what is the isomorphism?

2. Here is a nice characterization of cyclic groups.
Theorem: Let G be a finite group, and let $n = |G|$. Then the following are equivalent:

1. For every $d|n$, G has at most one cyclic subgroup of order d.

2. For every $d|n$, G has at least one cyclic subgroup of order d.

3. G is cyclic.

Prove this theorem.

HINT: Let $\mathcal{C}$ be the set of all cyclic subgroups of G. Let $\pi : G \to \mathcal{C}$ be the map sending every element $x \in G$ to the cyclic group it generates. Let m_d denote the number of cyclic subgroups of G, of order d. Using π to count the elements of G, establish the formula

$$n = \sum_{d|n} m_d \phi(d) \ . \qquad (1)$$

where ϕ is Euler's ϕ-function. (I.e., $\phi(d)$ is the number integers $0 < k < d$ such that k and d are relatively prime.) Get a second formula by applying (1) to the

special case of a cyclic group of order n. Prove the theorem by subtracting the two formulas.
DF 2.4.10, 2.4.11, 2.4.17, 3.1.32, 3.1.35, 3.1.36, 3.1.42, 3.1.43, 3.2.4, 3.2.9ef, 3.2.21, 3.3.4, 3.3.7, 3.3.9

MATH 8000 Homework 2, due Friday 8/28/09.

1. Let G be the group generated by elements x_i, $i = 1, 2$, subject to the relations

$$x_1^2 = x_2^2 = e \ , \ x_2 x_1 x_2 = x_1 x_2 x_1$$

G is a familiar group. Which one? (With proof)

2. Same as problem 1, with three elements x_i, $i = 1, 2, 3$, subject to relations

$$x_1^2 = x_2^2 = x_3^2 = e \ , \ x_1 x_3 = x_3 x_1 \ , \ x_2 x_1 x_2 = x_1 x_2 x_1 \ , \ x_3 x_2 x_3 = x_2 x_3 x_2$$

3. Prove that $\mathrm{Aut}(\mathbb{Q}) \simeq \mathbb{Q}^*$.

4. Prove that $\mathrm{Aut}(\mathbb{C}) \not\simeq \mathbb{C}^*$.

DF 1.3.12, 1.4.2, 1.6.4, 1.6.23, 1.7.10, 1.7.19, 1.7.21, 1.7.23, 2.1.6, 2.2.12def, 2.2.14

MATH 8000 Homework 1, due Friday 8/21/09.

1. Let X, Y and Z be sets, and let $f : X \to Y$ and $g : X \to Z$ be surjections. Say that f and g are equivalent if there exists a bijection $h : Y \to Z$ such that $h \circ f = g$.
i) Given a surjection $f : X \to Y$, write down an equivalence relation naturally associated to f.
ii) Given an equivalence relation $R \subset X \times X$, write down a partition naturally associated to R.
iii) Given a partition of $\mathcal{P}$ of X, write down a surjection naturally associated to $\mathcal{P}$.
iv) Prove that if you if you start with a surjection $f : X \to Y$ and and go around the loop just described, you return to an equivalent surjection.
DF:
0.2.1f, 0.3.8, 1.1.22, 1.1.25, 1.2.1 – 1.2.4, 1.2.12