Graduate Algebra
Homework 6
Due 2015-03-04

1. Let $n \geq 2$. For a ring $R$ define $GL(n, R)$ as the set of $n \times n$ matrices $M$ such that $M^{-1}$ is also in $M_{n \times n}(R)$.
   (a) Show that $GL(n, R) = \{ g \in M_{n \times n}(R) | \det(M) \in R^\times \}$.
   (b) Show that $GL(n, -)$ yields a covariant functor from the category of rings (with morphisms taking 1 to 1) to the category of sets.
   (c) Show that $GL(n, -)$ is representable.

Proof. (1): We know from lectures that a linear map is invertible iff its determinant is invertible.

(2): Suppose $f : R \to S$ is a ring homomorphism. Define $f : GL(n, R) \to GL(n, S)$ by $f((a_{i,j})) = (f(a_{i,j}))$. Since $f$ is a homomorphism we deduce that $\det(f((a_{i,j}))) = f(\det((a_{i,j})))$ and so $f$ takes invertible matrices to invertible matrices because $f : R^\times \to S^\times$. Note that $GL(n, -)$ respects compositions by definition and the identity yields the identity.

(3): Let $R = \mathbb{Z}[x_{i,j}|1 \leq i,j \leq n]/(y \det((x_{i,j})) - 1)$ and $M = (x_{i,j})$. Since $y \det M = 1$ it follows that $\det M \in R^\times$ so $M \in GL(n, R)$. I'll show that $GL(n, -)$ is represented by $R, M$. If $S$ is any ring we need to show that $\text{Hom}(R, S) \cong GL(n, S)$ is a bijection via $f \mapsto f(M)$. First, if $N \in GL(n, S)$ is any matrix define $f : \mathbb{Z}[x_{i,j}|i,j] \to S$ by $f(x_{i,j}) = n_{i,j}$ which can always be done. Next, since $f(\det((x_{i,j}))) = \det(N) \in S^\times$ it follows that $f$ factors through the localization $\mathbb{Z}[x_{i,j}|\det((x_{i,j}))] \cong R$. This proves surjectivity of the map.

For injectivity, suppose $f, g : R \to S$ yield the same matrix. Then $f(x_{i,j}) = g(x_{i,j})$ and so necessarily $f(y) = g(y)$ is the inverse of $\det(f(x_{i,j})) = \det(g(x_{i,j}))$. Since $R$ is generated by $x_{i,j}$ and $y$ it follows that $f = g$. \hfill \Box

2. (a) Suppose $L/K$ is a field extension such that $L$ has $p^m$ elements and $K$ has $p^n$ elements. Show that $m \mid n$.
   (b) Suppose $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ where $\alpha_i^2 \in \mathbb{Q}$ for $1 \leq i \leq n$. Show that $\sqrt{2} \notin K$. [Hint: The degree is multiplicative in towers of extensions.]

Proof. (1): Let $d = [L : K]$. Then $L \cong K^d$ and counting we get $p^n = (p^m)^d$ so $m \mid n$.

(2): We'll show by induction that if $K_n = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)/\mathbb{Q}$ then $[K_n : \mathbb{Q}] = 2^n$. The base case is trivial $K_0 = \mathbb{Q}$. Next, $K_n = K_{n-1}(\sqrt[n]{\alpha_n})$ which has minimal polynomial either linear or quadratic over $K_{n-1}$.

Thus $[K_n : K_{n-1}] \mid 2$ and so $[K_n : \mathbb{Q}] \mid 2^n$. Finally, if $\sqrt{2} \in K_n$ then $[K_n : \mathbb{Q}] = [K_n : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$ is divisible by 3 which cannot happen. \hfill \Box

3. In each of the following examples you are given a polynomial $P(X) \in K[X]$ over some field $K$. In each case find the splitting field of $P$ over $K$ as well as the degree over $K$ of the splitting field. The letter $p$ denotes a prime number.


(a) \( X^n - 2 \in \mathbb{Q}[X] \).

(b) \( X^{p-1} - t \in \mathbb{F}_p(t)[X] \) for \( p > 2 \).

(c) \( X^4 + X^2 + 1 \in \mathbb{Q}[X] \).

(d) \( X^n - t - 1 \in \mathbb{C}(t)[X] \). Here \( \mathbb{C}(t) \) is the fraction field of \( \mathbb{C}[t] \) consisting of Laurent series.

Proof. (1): The splitting field must contain all \( \zeta_p^k \sqrt{2} \) for \( 0 \leq k < p \). But then it must contain \( \sqrt{2} \) and \( \zeta_p \) and immediately the splitting field is \( K = \mathbb{Q}(\sqrt{2}, \zeta_p) \). Note that \( K \) is the composite of \( \mathbb{Q}(\sqrt{2}) \) of degree \( p \) over \( \mathbb{Q} \) and \( \mathbb{Q}(\zeta_p) \) of degree \( p-1 \) over \( \mathbb{Q} \) (because the minimal polynomial of \( \zeta_p \) is \( X^p - 1 \) which is irreducible over \( \mathbb{Q} \)). Since the two degrees are coprime the composite has degree the product \( p(p-1) \).

(2): Let \( K = \mathbb{F}_p(\sqrt[p]{-u}) \). I claim that \( K \) is the splitting field. Note that \( \mathbb{F}_p[x] \) is cyclic (proved last semester) and so every \( (p-1) \)-th root of unity is in \( \mathbb{F}_p \). Thus \( K \) contains all the roots of \( X^{p-1} - t \) and in fact \( X^{p-1} - t = \prod_{i=1}^{p-1}(X - i\sqrt[p]{-u}) \). For the degree \( [K : \mathbb{F}_p(t)] = p - 1 \) the degree of the minimal polynomial.

(3): \( X^4 + X^2 + 1 = (X^2 + 1) - X^2 = (X^2 + X + 1)(X^2 - X + 1) \). The splitting field is the composite of the splitting fields of the two polynomials, namely \( \mathbb{Q}(\sqrt{5}) \) and \( \mathbb{Q}(\sqrt{-5}) \). This splitting field is \( \mathbb{Q}(i, \sqrt{5}) \). It’s degree is \( 4 \) because the basis \( 1, \sqrt{5} \) is independent over \( \mathbb{Q}(i) \).

(4): Note that the roots are \( \zeta_n^k \sqrt{1+u} = \zeta_n^k \sum_{m \geq 0} (\sqrt[n]{m})t^m \in \mathbb{C}(t) \) so the splitting field is \( \mathbb{C}(t) \). \( \square \)

4. Let \( K \) be a field and \( K(x) \) be the field of rational functions with coefficients in \( K \). Let \( P(x), Q(x) \in K[x] \) be two coprime polynomials and \( t = P/Q \in K(x) \).

(a) Show that \( P(X) - tQ(X) \in K(t)[X] \) is irreducible and has \( X = x \) as a root. [Hint: Use Gauss' lemma and the fact that \( K[X][t] = K[t][X] \).]

(b) Conclude that \( [K(x) : K(t)] = \max(\deg(P), \deg(Q)) \).

Proof. (1): Gauss’ lemma says that \( P(X) - tQ(X) \) is irreducible over \( K(t) \) if and only if \( P(X) - tQ(X) \) is irreducible over \( K[t] \). If it’s reducible over \( K[t][X] \) then it’s also reducible over \( K[X][t] = K[t][X] \). But it is linear in \( X \) and so the only way to be reducible is if \( P(X) - tQ(X) \) is divisible by a polynomial in \( X \). But this contradicts that \( P \) and \( Q \) are coprime. Finally, \( P(x) - tQ(x) = 0 \) by definition of \( t \).

(2): The minimal polynomial of \( x \) over \( K(t) \) is the irreducible polynomial \( P(X) - tQ(X) \) of degree \( \max(\deg(P), \deg(Q)) \). The same is therefore true of \( [K(x) : K(t)] \). \( \square \)

5. Suppose \( L/K \) is a finite extension of fields and \( K \subset M_1, M_2 \subset L \) are two subextensions. Show that \( M_1 \otimes_K M_2 \) is a field if and only if \( [M_1M_2 : K] = [M_1 : K][M_2 : K] \). [Hint: Look at the multiplication map \( M_1 \otimes_K M_2 \to M_1M_2 \).

Proof. Look at \( m : M_1 \otimes_K M_2 \to M_1M_2 \) given by \( m(\sum x_i \otimes y_i) = \sum x_iy_i \). This is a homomorphism of \( K \)-modules. Defining \( (x \otimes y) \cdot (x' \otimes y') = (xx') \otimes (yy') \) we get a \( K \)-algebra structure on \( M_1 \otimes_K M_2 \) and one can check that \( m \) is a \( K \)-algebra homomorphism which sends \( 1 \) to \( 1 \).

If \( M_1 \otimes_K M_2 \) is a field then \( m \) is a field homomorphism which is not trivial as it send \( 1 \) to \( 1 \). Thus \( m \) is injective and so \( \dim_K M_1 \otimes_K M_2 \leq \dim_K M_1 M_2 \). But LHS is \( [M_1 : M][M_2 : K] \) and the RHS is always \( \leq [M_1 : K][M_2 : K] \) from class. Thus equality occurs. 

Suppose now that equality occurs. Elements of \( M_1M_2 \) are rational expressions in elements of \( M_1 \) and \( M_2 \). Since \( M_1M_2/K \) is finite these rational expressions are algebraic elements and therefore they are polynomial expressions in elements of \( M_1 \) and \( M_2 \). Collecting terms we deduce that every element of \( M_1M_2 \) is of the form \( \sum x_iy_i = m(\sum x_i \otimes y_i) \) for \( x_i \in M_1 \) and \( y_i \in M_2 \). Thus \( m \) is surjective. Since the LHS and RHS have equal dimension over \( K \) and \( m \) is a \( K \)-vector space surjective homomorphism we deduce it is an isomorphism and therefore \( M_1 \otimes_K M_2 \cong M_1M_2 \) is a field. \( \square \)