Solutions to Homework 8

Math 601, Spring 2008

33) (10 points). Let K be an infinite field. Show that $K^\times$ is not cyclic.

We prove the contrapostion: $K^\times$ cyclic implies K finite. Let F be the prime subfield of K, and let a be a generator of the cyclic group $K^\times$. Clearly $K = F(a)$. Since $F^\times \subset K^\times$ is cyclic, and $\mathbb{Q}^\times$ is not cyclic we see that F is finite. Moreover a has to be algebraic over F because the multiplicative group of nonzero rational functions, $F(X)^\times$, is clearly not cyclic. Thus the finiteness of F and $[K : F]$ implies the finiteness of K.

34) (10 points). Show that $\mathrm{Aut}(R) = 1$.

This is the same problem as Problem 3b) from HW1 of Math600, which is reproduced below with solution.

Problem: Suppose $f : \mathbb{R} \to \mathbb{R}$ is a function which satisfies $f(x + y) = f(x) + f(y)$ and $f(xy) = f(x)f(y)$, for all $x, y \in \mathbb{R}$. Show that either $f \equiv 0$, or that f is the identity map.

Solution: By $f(1) = f(1)^2$, it follows that $f(1) = 0$ or 1. In the former case $f \equiv 0$. Now, suppose $f(1) = 1$. We easily deduce that $f_{|\mathbb{Q}} = id$. Now we make a (tricky) observation that $x > 0 \Rightarrow f(x) > 0$. To see this, for $x > 0$, we have $f(x) = f(\sqrt{x})^2 > 0$. Thus f is strictly increasing. Now suppose $x \neq f(x)$, we may assume $x < f(x)$ by replacing x with $-x$ if necessary. We, pick a rational number y with $x < y < f(x)$ and apply f to the left inequality to infer $f(x) < f(y) = y$ which contradicts the right inequality. This contradiction shows that $f(x) = x$ for all $x \in \mathbb{R}$

35 [D-F], 13.6 #13 (10 points). (A finite division ring is a field.)

a) Clearly Z is a division subring of D, and it is commutative hence it is a finite field $\mathbb{F}_q$, where $q = p^N$ and p is the characteristic of Z. Since D is finite, it is a finite dimensional vector space over the field Z and hence has q^n elements.

b) For $x \in D^\times = D - \{0\}$, the centralizer $Z(x)$ is a division subring of D containing Z, and for

the same reason as above, has q^m elements. The equality $m = n$ holds iff $x \in Z$, thus $m < n$ if $x \notin Z$.

c) The cardinality of $Z^\times$ is $q-1$ and that of $D^\times$ is $q^n - 1$. Let $\{x_1, \cdots x_r\}$ denote representatives of the conjugacy classes of the finite group $D^\times$. The stabilizer of x_i under the conjugation action of $D^\times$ on itself, is $Z(x_i)$ of order q^{m_i}, as shown above. The class equation for $D^\times$ thus reads:

$$q^n - 1 = q - 1 + \sum_{i=1}^{r} \frac{q^n - 1}{q^{m_i} - 1} \tag{1}$$

d) By the elementary problems 13.5.[3-4] of [D-F], the fact that index $[D^\times : Z(x_i)] = \frac{q^n-1}{q^{m_i}-1}$ is an integer implies that $m_i \,|\, n$, and that $X^{m_i} - 1 \,|\, X^n - 1$. Also, $m_i \neq n$ because none of the x_i's are in Z. We have :

$$\frac{X^n - 1}{\Phi_n(X)(X^{m_i} - 1)} = \frac{\prod_{d|n, d<n} \Phi_d(X)}{\prod_{d'|m_i} \Phi_{d'}(X)}$$

and clearly the rhs in the equation above is a polynomial, since $\{d'|m_i\} \subset \{d|n, d < n\}$, and thus evaluating at q we get that $\frac{q^n-1}{\Phi_n(q)(q^{m_i}-1)}$ is an integer.

e) Thus, in the class equation (1) above, both the lhs and the second term of the rhs are divisible by $\Phi_n(q)$ and hence $\Phi_n(q) \,|\, q-1$. From the expansion $\Phi_n(q) = \prod_{\xi \text{ primtv}} (q - \xi)$ and the elementary fact that the abolute value $|q - \xi| > q - 1$ if $n > 1$ (and $\xi \neq 1$), we see that $\Phi_n(q) \,|\, q - 1$ is possible only if $n = 1$. Thus D and Z have the same cardinality, and hence D is the finite field $Z \simeq \mathbb{F}_q$.

36 [D-F], 13.6 #14-15-16 (10 points). (Special Case of Dirichlet's theorem on primes in Arithmetic Progression.)

Sketch: Suppose the set of primes dividing $\{P(n) \mid n \geq 1\}$ is finite and equal to $\{p_1, \cdots, p_k\}$. Then $P(N + ap_1p_2 \cdots p_k x) \equiv p(N) = a \bmod (ap_1p_2 \cdots p_k)$, thus we deduce that $Q(x) = a^{-1}P(N + ap_1p_2 \cdots p_k x)$ has integer coefficients, and also that $Q(n) \equiv 1 \bmod (p_1p_2 \cdots p_k)$. Therefore, for almost any M, $Q(M)$ has a prime factor p' different from $p_1, \cdots, p_k$, and hence so does $P(N + ap_1p_2 \cdots p_k M) = aQ(M)$. This contradiction shows that the set of primes dividing $\{P(n) \mid n \geq 1\}$ is infinite.

Suppose, p is an odd prime with $(p, m) = 1$ and let $a \in \mathbb{Z}$ (different from the a above) with $\Phi_m(a) = 0 \bmod (p)$, then $\Phi_m(X) | X^m - 1$ implies $a^m - 1 = 0 \bmod (p)$, so that $(a, p) = 1$. Suppose d is the order of a in $\mathbb{F}_p^\times$ and d is a proper divisor of m. We observe that $\Phi_m(X)(X^d - 1) = \Phi_m(X) \prod_{e|d} \Phi_e(X)$ is a divisor of $X^m - 1$, so that a is a multiple root of $X^m - 1 \bmod (p)$. But this

implies $ma^{m-1} \equiv 0 \bmod (p)$ and multiplying by a we get $p|m$, a contradiction. Thus the order of a in $\mathbb{F}_p^\times$ is m, and this implies $m|p-1$ or equivalently $p \equiv 1 \bmod (m)$.
Thus we have shown that if p is an odd prime with $p|\Phi_m(a)$, then either $p|m$ or $p \equiv 1 \bmod (m)$. Since there are infinitely many primes dividing $\Phi_m(a)$ as a runs through the positive integers (as shown above) and only finitely many of these satisfy $p|m$, we must have $p \equiv 1 \bmod (m)$ for infinitely many primes.

37 [D-F], 14.1 #8 (10 points) Prove that $\mathrm{Aut}_k(k(X)) = \mathrm{PGL}(2,k)$.

We give two proofs, the first one being more geometric and the second one algebraic.

Proof 1: Let $\mathbb{P}^1$ denote the set of lines passing through the origin of the affine space $\mathbb{A}^2(k) = \{(X_1, X_2) \mid X_i \in k\}$. We can view $\mathbb{P}^1$ as $k \cup \infty$ where k corresponds to the lines which intersect $X_1 = 1$, and ∞ is the line $X_1 = 0$. In other words $X \in k$ corresponds to $(1 : X)$ and $X = \infty$ corresponds to $(0 : 1)$. A polynomial $g(X_1, X_2)$ is homogeneous of degree n, if $p(\lambda X_1, \lambda X_2) = \lambda^n p(X_1, X_2)$ for all $\lambda \in k^\times$. We define the ring of projective transformations:

$$R = \{G : (X_1 : X_2) \mapsto (g_1(X_1, X_2) : g_2(X_1, X_2)) \mid g_1, g_2 \text{ are homogeneous of same degree}\}$$

Multiplication in R is composition of transformations and addition is $G + F : (X_1 : X_2) \mapsto (g_1 f_2 + f_1 g_2 : f_1 f_2)$. Let S be the ring $S := \mathrm{End}_k(k(X))$. Given $G \in R$ let $X = X_2/X_1$, this determines an element $g \in S$ by $X \mapsto g(X) = g_2(X_1, X_1X)/g_1(X_1, X_1X)$. Conversely given an element $g \in S$, $X \mapsto g(X)$, we set $X = X_2/X_1$ and obtain (by clearing denominators) an element $G \in R$. These two maps are inverses of each other, hence we have shown that $G \mapsto g$ is an isomorphism between R and S. On the level of units, we thus have an isomorphism of groups $\mathrm{Aut}(\mathbb{P}^1) := R^\times \to \mathrm{Aut}_k(k(X))$.

Now $\mathrm{PGL}(2,k) \subset \mathrm{Aut}(\mathbb{P}^1)$, and given three distinct points $p, q, r \in \mathbb{P}^1$, it is a standard fact that there is a $\sigma \in \mathrm{PGL}(2,k)$ such that σ sends p, q, r to $0, 1, \infty$ $(= (1:0), (1:1), (0:1))$ respectively. (This can be done over any field since the entries of a matrix of σ are rational functions of p, q, r). Thus given $G \in \mathrm{Aut}(\mathbb{P}^1)$, by composing with such a σ, we may suppose G fixes $0, 1, \infty$. Thus we may write $g : X \mapsto Xa(X)/b(X)$, with $a(X), b(X)$ being polynomials satisfying $a(1) = b(1) = 1$ (so that G fixes 1), $b(0) \neq 0$ (so that G fixes 0) and $\deg(b) < 1 + \deg(a)$ (so that G fixes ∞). In fact $b(X)$ has to be identically 1. To see this, let α be a root of an irreducible factor of $b(X)$ in some extension field $k(\alpha)$. Note that the irreducible polynomial (in the variable T) of α over the fields k and $k(X)$ is the same, hence the k-linear isomorphism $g : k(X) \to k(X)$ extends to an isomorphism $g' : k(\alpha)(X) \to k(\alpha)(X)$ given by the same rule $X \mapsto g(X)$, and by the above

discussion corresponds to an element of $G' \in \mathrm{Aut}(\mathbb{P}^1(k(\alpha)))$. However G' sends both α and ∞ to ∞ and hence is not invertible. This contradiction shows that $b(X) \equiv 1$ and therefore, $g : X \mapsto Xa(X)$ with $a(1) = 1$. Clearly the degree of any nonconstant polynomial in $k(g(X)))$ has degree at least 1+deg(a), therefore $k(X) = k(g(X))$ requires deg$(a) = 0$ and together with $a(1) = 1$ this implies $a(X) = 1$ and $g(X) = X$. This shows that $\mathrm{Aut}_k(k(X)) = \mathrm{PGL}(2, k)$.

Proof 2: For $p(X), q(X)$ relatively prime, let $Y = p(X)/q(X)$. The extension $k(X)$ of $k(Y)$ is generated by X whose irreducible polynomial over $k(Y)$ in the variable T is $p(T) - Yq(T)$. To see that this, we note that $p(T) - Yq(T)$ is certainly irreducible in $k(T)[Y]$ and hence in $k[T, Y]$ (because $p(T), q(T)$ are rel. prime) and hence in $k(Y)[T]$. Also the degree in T of $p(T) - Yq(T)$ is max $\{$ deg(p), deg$(q)\}$. So for $k(Y) = k(X)$ we need that the degrees of both p and q are atmost one, and thus we get a fractional linear transformation $Y = \frac{aX+b}{cX+d}$ which is invertible iff $ad - bc \neq 0$. Thus we have shown that $\mathrm{Aut}_k(k(X)) = \mathrm{PGL}(2, k)$.