Homework 9

Aleck Zhao

April 14, 2017

1. Let F be a field, and define projective n-space $\mathbb{P}^n(F)$ to be the set of 1-dimensional F-subspaces in F^{n+1}. Give a group G and a G-set X such that the set of orbits for the action is in natural bijection with $\mathbb{P}^n(F)$. When F is a finite field with q elements, deduce from this that

$$\#\mathbb{P}^n(F) = \frac{q^{n+1}-1}{q-1}$$

Solution. Consider the group $G = F^\times$ and the set $X = F^{n+1} \setminus 0$. Then the orbits are exactly the 1-dimensional F subspaces of F^{n+1}. If $\#F = q$, then by the orbit decomposition theorem, we have

$$\#X = \#X_f + \sum_{i=1}^{n} \#(G \cdot x_i)$$

Here, X_f is empty because nothing in $F^{n+1} \setminus 0$ is fixed by every element in F, and $\#X = q^{n+1} - 1$. Then $\#(G \cdot x_i) = q - 1$ because if $a, b \in G$ and $x_i = (g_1, \cdots, g_{n+1})$, then

$$\begin{aligned} a \cdot (g_1, \cdots, g_{n+1}) = (ag_1, \cdots, ag_{n+1}) = (bg_1, \cdots, bg_{n+1}) = b \cdot (g_1, \cdots, g_{n+1}) \\ \iff ag_i = bg_i, \forall i \\ \iff a = b \end{aligned}$$

Thus, we have

$$\begin{aligned} q^{n+1} - 1 &= 0 + \sum_{i=1}^{n} (q-1) = n(q-1) \\ \implies n &= \frac{q^{n+1}-1}{q-1} \end{aligned}$$

where n is the number of orbits, which is equal to $\#\mathbb{P}^n(F)$, as desired. □

Section 10.1: Galois Groups and Separability

2. Prove: If $E \supseteq F$ are fields, $G = \mathrm{Aut}_F(E), u \in E$, and $\sigma \in G$, then

(1) $\sigma[f(u)] = f[\sigma(u)]$ for all $f \in F[x]$.

Proof. Let $f = a_0 + a_1x_1 + \cdots + a_nx^n$ with $a_0, \cdots, a_n \in F$. Then since $\sigma \in \mathrm{Aut}_F(E)$, it must fix F, so $\sigma(a_i) = a_i$ for all i. Then

$$\begin{aligned} \sigma[f(u)] &= \sigma(a_0 + a_1u + \cdots + a_nu^n) = \sigma(a_0) + \sigma(a_1u) + \cdots + \sigma(a_nu^n) \\ &= \sigma(a_0) + \sigma(a_1)\sigma(u) + \cdots + \sigma(a_n)\sigma(u)^n \\ &= a_0 + a_1\sigma(u) + \cdots + a_n\sigma(u)^n \\ &= f[\sigma(u)] \end{aligned}$$

□

(2) In particular, if u is a root of f, then $\sigma(u)$ is also a root of f.

Proof. If u is a root of f, then $f(u) = 0$, so

$$f[\sigma(u)] = \sigma[f(u)] = \sigma(0) = 0$$

so $\sigma(u)$ is also a root of f. □

(3) If u is algebraic over F, and $\sigma, \tau \in \mathrm{Aut}_F(F(u))$, then $\sigma = \tau$ if and only if $\sigma(u) = \tau(u)$.

Proof. $(\implies)$: This is trivial. If two maps are the same, then they send u to the same thing. $(\impliedby)$: Since $F(u) = \{ f(u) \mid f \in F[x] \}$, we have

$$\begin{aligned} \sigma``(F(u)) &= \{ \sigma[f(u)] \mid f \in F[x] \} = \{ f[\sigma(u)] \mid f \in F[x] \} \\ &= \{ f[\tau(u)] \mid f \in F[x] \} = \{ \tau[f(u)] \mid f \in F[x] \} \\ &= \tau``(F(u)) \end{aligned}$$

so $\sigma = \tau$. □

13. If $E = \mathbb{Q}(\sqrt[4]{2}, i)$, show that $\mathrm{Aut}_{\mathbb{Q}}(E) \cong D_4$.

Proof. Let $u = \sqrt[4]{2}$. Then the minimal polynomials of u and i are $x^4 - 2$ and $x^2 + 1$, respectively, with roots $\{u, -u, iu, -iu\}$ and $\{i, -i\}$, respectively. Then any $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(E)$ must have $\sigma(u) \in \{u, -u, iu, -iu\}$ and $\sigma(i) \in \{i, -i\}$. So we may find $\sigma, \tau \in \mathrm{Aut}_{\mathbb{Q}}(E)$ such that $\sigma(u) = iu, \sigma(i) = i$ and $\tau(u) = u, \tau(i) = -i$. Then $o(\sigma) = 4$ and $o(\tau) = 2$, and

$$\begin{aligned} \sigma\tau\sigma(u) &= \sigma\tau(iu) = \sigma\tau(i)\sigma\tau(u) \\ &= \sigma(-i)\sigma(u) = -\sigma(i)\sigma(u) = (-i)(iu) = u \\ \tau(u) &= u \end{aligned}$$

so $\langle \sigma, \tau \rangle = \mathrm{Aut}_{\mathbb{Q}}(E) \cong D_4$, as desired. □

20. Let $F = K(t)$ denote the field of rational forms over a field K in an indeterminate t. Show that $x^2 - t$ is irreducible over F but is not separable if $\operatorname{char} K = 2$.

Proof. Suppose $x^2 - t = (x - a)(x - b)$ for $a, b \in K(t)$. Then comparing coefficients, we have

$$\begin{aligned} a + b &= 0 \\ ab &= -t \\ \implies a^2 &= t \end{aligned}$$

Now, if $a = p/q$ for $p, q \in K[t]$, then $t = a^2 = p^2/q^2 \implies tq^2 = p^2$. However, $\deg p^2$ is even and $\deg tq^2$ is odd, so this is impossible. Thus $x^2 - t$ is irreducible. If $\operatorname{char} K = 2$, then $(x^2 - t)' = 2x \equiv 0$, so $x^2 - t$ would not be separable. □

22. (a) Show that the following are equivalent for a polynomial $f \in F[x;]$.

(1) f has no repeated root in any extension field of f.

(2) f has no repeated root in some splitting field over F.

(3) f and f' are relatively prime in $F[x]$.

Proof. ($1 \implies 2$) : This is trivial, since splitting fields are extension fields.

($2 \implies 3$) : Suppose f splits in a splitting field E. If f and f' were not relatively prime in $F[x]$, then there exists some $d \in F[x]$ such that $d \mid f$ and $d \mid f'$ where $\deg d \geq 1$. Since $d \mid f$, it must also split in E, so suppose d has a root $u \in E$. Then $(x-u) \mid d$ so $(x-u) \mid f$ and $(x-u) \mid f'$, so it must be the case that $(x-u)^2 \mid f$, and thus f has a repeated root. This is a contradiction, so f and f' are relatively prime.

($3 \implies 1$) : If f has a repeated root u in some extension field E of f. Then $(x-u)^2 \mid f \iff (x-u) \mid f, f'$. If f and f' are relatively prime, then $1 = fg + f'h$ for some $g, h \in F[x]$. Since E is an extension field of F, this equation also holds in E. Now, we have $1 = f(u)g(u) + f'(u)h(u) = 0$, a contradiction, so f has no repeated roots in any extension field. □

(b) If f is as in (a), show that f is separable, but not conversely.

Proof. If f was not separable, then one of its irreducible factors is not separable, say $p \in F[x]$. If $f = pg$ for $g \in F[x]$, then $f' = pg' + p'g$, and since p is not separable, $p' = 0$, so $f' = pg'$. Then $\gcd(f, f') = p$, so f and f' are not relatively prime, which contradicts (3). Thus, f is separable.

However, consider $f = (x-1)^2$. Then f is separable because its irreducible factors are both $(x-1)$, which are both separable. However, f has a repeated root, contradicting (1). □

25. If $E \supseteq F$ and $f \in F[x]$ is separable over F, show that f is separable over E.

Proof. Suppose $f = pg$ for some irreducible $p \in E[x]$. Since f is separable over F, all of its irreducible factors must be separable. Suppose $f = q_1 \cdots q_r$ for irreducible and separable $q_i \in F[x]$. Then since E is an extension field of F, this factorization holds in E as well. Then $f = pg = q_1 \cdots q_r$ in $E[x]$, and since p is irreducible in $E[x]$ is it prime, so we must have $p \mid q_i$ for some i. If p was not separable, then it would have a repeated root in E, but then q_i would also have a repeated root in E, which is an extension field of F, which would mean q_i is not separable. This is a contradiction, so p is separable in E, so f is separable in E, as desired. □

26. If $E \supseteq K \supseteq F$ and $E \supseteq F$ is a separable extension, show that both $E \supseteq K$ and $K \supseteq F$ are separable extensions.

Proof. Since $E \supseteq F$ is separable, every $u \in E$ has a separable minimal polynomial over F. Since $K \supseteq E$, it follows that every $u \in K$ also has a separable minimal polynomial over F, so $K \supseteq F$ is a separable extension.

For $u \in E$, let the minimal polynomial of u over F be f, and the minimal polynomial over K be k. Then it follows that $k \mid f$ in $E[x]$, and since f is separable, k must also be separable, and thus $E \supseteq K$ is a separable extension. □

27. Let F have characteristic p. If $f = x^p - a$ where $a \in F$, show that f is irreducible or a power of a linear polynomial. (Hint: Lemma 5 and Theorem 4)

Proof. Let f have a root u in some extension field E. Then $f(u) = u^p - a = 0 \implies u^p = a$, so we have $f = x^p - u^p = (x-u)^p$ since $\operatorname{char} F = p$. If f is not irreducible, then this is its factorization in $F[x]$, so then f is a power of a linear polynomial.

If f is not a power of a linear polynomial, then it must be that $u \notin F$, so $F(u)$ is a splitting field of f over F. Suppose f has a nontrivial irreducible factor $g \in F[x]$. Then $g = (x-u)^q$ for some $1 < q < p$, since $u \notin F$. Then since g has a repeated root u, we must have $g' \equiv 0$ by Lemma 5, so g is not separable, and thus $g = h(x^p)$ by Theorem 4, for some $h \in F[x]$. Since every irreducible factor of f takes this form, we have

$$f = h_1(x^p) \cdots h_r(x^p) = x^p - a$$

Thus we must have $h_i(x^p) = x^p - a$ for some i and the rest are 1, so f is irreducible. □