Homework 7

Aleck Zhao

April 2, 2017

1. Let R be a ring, and let σ be an automorphism of R. Show that $\{ a \in R \mid \sigma(a) = a \}$ is a subring of R, and a subfield if R is a field.

   Proof. Call the subset S. Any automorphism must fix 1, so $1 \in S$. Now if $a, b \in S$, we have

   $$\sigma(a+b) = \sigma(a) + \sigma(b) = a + b$$
   $$\sigma(ab) = \sigma(a)\sigma(b) = ab$$

   so $a + b, ab \in S$, so S is indeed a subring. Now, if R is a field, then for all nonzero $a \in R$,

   $$1 = \sigma(1) = \sigma\left(a \cdot \frac{1}{a}\right) = \sigma(a)\sigma\left(\frac{1}{a}\right)$$

   Now, if $a \in S$, then $\sigma(a) = a$, so

   $$\sigma\left(\frac{1}{a}\right) = \frac{1}{\sigma(a)} = \frac{1}{a}$$

   so $\frac{1}{a} \in S$ as well, and thus S is a field. □

2. Let F be a finite field with p^n elements for p a prime. Show that each element $a \in F$ has a pth root in F, i.e. there exists $b \in F$ such that $b^p = a$. Is b unique? By contrast, for $K := F(x)$ the fraction field of the polynomial ring $F[x]$, show that x has no pth root in K.

   Proof. Since $F = \mathbb{F}_{p^n}$ is the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$, we have $a^{p^n} = a$ for all $a \in \mathbb{F}_{p^n}$. Thus, if $b = a^{p^{n-1}}$, we have

   $$b^p = (a^{p^{n-1}})^p = a^{p^n} = a$$

   so b is a pth root of a. If $b^p = c^p = a$, then $\left(\frac{b}{c}\right)^p = 1$. The nonzero elements of F form a cyclic group of order $p^n - 1$, so since $\gcd(p, p^n - 1) = 1$, it must be the case that $b/c = 1 \implies b = c$ so the pth root is unique.

   Suppose x had a pth root in K, so that for some $f, g \in F[x]$, we have $x = \left(\frac{f}{g}\right)^p$. Then $g^p x = f^p$. Note that $a^p \neq 0$ for any $0 \neq a \in F$ since F is a field and therefore an integral domain. Thus, if $\deg f = m, \deg g = n$, we have $\deg(g^p x) = pn + 1 = pm = \deg f^p$ which is clearly impossible. Thus, there is no pth root of x, as desired. □

Section 6.4: Finite Fields

8. Find $[\mathbb{F}_{p^n} : \mathbb{F}_{p^m}]$ where $m \mid n$.

   Solution. We have

   $$\begin{aligned} [\mathbb{F}_{p^n} : \mathbb{F}_p] &= [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}][\mathbb{F}_{p^m} : \mathbb{F}_p] \\ \implies n &= [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] \cdot m \\ \implies \frac{n}{m} &= [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] \end{aligned}$$

   □

18. (a) Show that a monic irreducible polynomial $f \in F[x]$ has no repeated root in any splitting field over F if and only if $f' \not\equiv 0$ in $F[x]$.

Proof. ($\Longrightarrow$) : Suppose f has no repeated roots in E a splitting field of f over F, but that $f' \equiv 0$. Then if $a \in E$ where $(x-a) \mid f$, since $(x-a) \mid 0 \equiv f'$, so a is a repeated root of f in E, contradiction.

($\Longleftarrow$) : Now if $f' \not\equiv 0$, let $F[x] \ni g = \gcd(f, f')$. Then since f is irreducible, we must have either $g \equiv 1$ or $g = f$. The case $g = f$ is impossible because $g \mid f'$ so $f \mid f'$, but since $\deg f \geq \deg f'$, it must be that $f = f' \equiv 0$, which is contrary to assumption. Then $g \equiv 1$, so f and f', don't share any common factors. Thus, by Theorem 3, it can't have any repeated roots in any splitting field over F. □

(b) If $\operatorname{char} F = 0$, show that no irreducible polynomial has a repeated root in any splitting field over F.

Proof. Let $f \in F[x]$ be irreducible. If $\operatorname{char} F = 0$, we have $f' \equiv 0 \iff \deg f = 0$, which obviously has no repeated roots in any splitting field. Otherwise, $f' \not\equiv 0$ for any f with degree at least 1. Then by the result of (a), it follows that f has no repeated root in any splitting field over F. Since f was arbitrary, no irreducible polynomial has a repeated root in any splitting field over F. □

19. If $\operatorname{char} F = p$, show that a monic irreducible polynomial $f \in F[x]$ has a repeated root in some splitting field if and only if $f = g(x^p)$ for some $g \in F[x]$. (Hint: Ex 18)

Proof. ($\Longrightarrow$) : From Ex 18(a), if f has a repeated root in some splitting field, then we must have $f' \equiv 0$ in $F[x]$. Let

$$\begin{aligned} f &= a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n \\ f' &= a_1 + 2a_2 x + \cdots + (n-1)a_{n-1}x^{n-2} + nx^{n-1} \end{aligned}$$

If $f' \equiv 0$, then we must have $p \mid ka_k$ for all $1 \leq k \leq n-1$. Thus, if $p \nmid k$, we must have $a_k = 0$, which is exactly to say that all exponents of f are divisible by p, and all other coefficients are 0. Thus, $f = g(x^p)$, as desired.

($\Longleftarrow$) : If $f = g(x^p)$, then $f' = px^{p-1}g'(x^p) \equiv 0$ in F. Thus, if f has a root a in a splitting field E over F, then $(x-a) \mid f$ and $(x-a) \mid 0 \equiv f'$, so $(x-a)^2 \mid f$ by Theorem 3, so f has a repeated root in some splitting field of F. □

21. Let p be a prime and write $f = x^p - x - 1$. Show that the splitting field of f over $\mathbb{F}_p$ is $\mathbb{F}_p(u)$, where u is any root of f. (Hint: Compute $f(u+a), a \in \mathbb{F}_p$)

Proof. Let $a \in \mathbb{F}_p$. Now consider $f(u+a)$:

$$\begin{aligned} f(u+a) &= (u+a)^p - (u+a) - 1 \\ &= u^p + a^p - u - a - 1 = (u^p - u - 1) + a^p - a \end{aligned}$$

Now, u is a root of f so the first term vanishes. Since $\left|\mathbb{F}_p^\times\right| = p - 1$ as a multiplicative group, it follows that $a^p - a = 0$. Thus, $u + a$ is a root of f for all $a \in \mathbb{F}_p$. Since $\deg f = p$, we must have f splits into p linear factors $[x - (u+a)]$ for each $a \in \mathbb{F}_p$. Then the splitting field is produced by adjoining each of $u + a$ to $\mathbb{F}_p$, but since $a \in \mathbb{F}_p$, this is just $\mathbb{F}_p(u)$, as desired. □

22. (a) Let f be a monic irreducible polynomial of degree n in $\mathbb{F}_p[x]$. Show that f divides $x^{p^n} - x$ in $\mathbb{F}_p[x]$. (Hint: First work over $\mathbb{F}_p(u)$, $f(u) = 0$. Use the uniqueness in Theorem 4 § 4.1.)

Proof. Since f is irreducible in $\mathbb{F}_p[x]$, it can't have any root in $\mathbb{F}_p$ since otherwise f would have a linear factor. Let u be a root of f in some extension E over $\mathbb{F}_p$. Then since f is irreducible and monic, it is the minimal polynomial of u, so $[E : \mathbb{F}_p] = n \implies |E| = p^n \implies E \cong \mathbb{F}_{p^n}$. Since $u \in E = \mathbb{F}_{p^n}$, it is a root of $x^{p^n} - x$. Now, let $x^{p^n} - x = fg + h$ where $g, h \in \mathbb{F}_p[x]$ and $0 \leq \deg h < n$. Now, letting $x = u$ (via the evaluation homomorphism), we have $u^{p^n} - u = 0 = f(u)g(u) + h(u) = h(u)$, so u is a root of h. However, since f was the minimal polynomial of u, it must be that $h \equiv 0$, so $f \mid (x^{p^n} - x)$, as desired. □

(b) Show that the degree of each monic irreducible divisor f of $x^{p^n} - x$ is a divisor of n. (Hint: Theorem 5)

Proof. Let f be a monic irreducible divisor of $x^{p^n} - x$, and let u be a root of f in some extension E. From above, we had $E = \mathbb{F}_{p^n}$, and since E is a field extension of $\mathbb{F}_p(u)$, we must have $\mathbb{F}_p(u) \cong \mathbb{F}_{p^m}$ for some $m \mid n$. Thus, $[\mathbb{F}_p(u) : \mathbb{F}_p] = m = \deg f$ since f is monic and irreducible and therefore the minimal polynomial, so $(\deg f) \mid n$, as desired. □

(c) Factor $x^8 - x$ into irreducibles in $\mathbb{F}_2[x]$.

Solution. We have $f = x^8 - x = x^{2^3} - x$, so the degree of each irreducible divisor of f has degree either 1 or 3. We have

$$x^8 - x = x(x^7 - 1) = x(x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$$

By inspection, the degree 6 polynomial has no roots in $\mathbb{F}_p$, so it must split into two irreducible degree 3 polynomials. Suppose one of them is $g = x^3 + ax^2 + bx + 1$. If $a = b = 0$ then $g(1) = 0$ and likewise if $a = b = 1$. Thus, either $a = 1$ and $b = 0$ or $a = 0$ and $b = 1$, so the factorization is given by

$$x^8 - x = x(x-1)(x^3 + x^2 + 1)(x^3 + x + 1)$$

□

Section 4.5: Symmetric Polynomials

14. Given $\sigma \in S_n$, define $\theta_\sigma : R[x_1, \cdots, x_n] \to R[x_1, \cdots, x_n]$ by $\theta_\sigma\left[f(x_1, \cdots, x_n)\right] = f(x_{\sigma 1}, \cdots, x_{\sigma n})$.

(a) Show that θ_σ is a ring automorphism of $R[x_1, \cdots, x_n]$.

Proof. First we show this is a ring homomorphism. Clearly $\theta_\sigma(1) = 1$. Now, for $f, g \in R[x_1, \cdots, x_n]$,

$$\begin{aligned}
\theta_\sigma\left[f(x_1, \cdots, x_n) + g(x_1, \cdots, x_n)\right] &= \theta_\sigma\left[(f+g)(x_1, \cdots, x_n)\right] \\
&= (f+g)(x_{\sigma 1}, \cdots, x_{\sigma n}) \\
&= f(x_{\sigma 1}, \cdots, x_{\sigma n}) + g(x_{\sigma 1}, \cdots, x_{\sigma n}) \\
&= \theta_\sigma(f) + \theta_\sigma(g) \\
\theta_\sigma\left[f(x_1, \cdots, x_n) \cdot g(x_1, \cdots, x_n)\right] &= \theta_\sigma\left[(fg)(x_1, \cdots, x_n)\right] \\
&= (fg)(x_{\sigma 1}, \cdots, x_{\sigma n}) \\
&= f(x_{\sigma 1}, \cdots, x_{\sigma n}) \cdot g(x_{\sigma 1}, \cdots, x_{\sigma n}) \\
&= \theta_\sigma(f) \cdot \theta_\sigma(g)
\end{aligned}$$

Now if

$$\theta_\sigma(f) = f(x_{\sigma 1}, \cdots, x_{\sigma n}) = g(x_{\sigma 1}, \cdots, x_{\sigma n}) = \theta_\sigma(g)$$

then consider σ^{-1} and its associated $\theta_{\sigma^{-1}}$. Then applying $\theta_{\sigma^{-1}}$ to both of these polynomials,

$$\begin{aligned}&\theta_{\sigma^{-1}}\left[f(x_{\sigma 1},\cdots,x_{\sigma n})\right]=f(x_{\sigma^{-1}\sigma 1},\cdots,x_{\sigma^{-1}\sigma n})=f(x_1,\cdots,x_n)\\=&\theta_{\sigma^{-1}}\left[g(x_{\sigma 1},\cdots,x_{\sigma n})\right]=g(x_{\sigma^{-1}\sigma 1},\cdots,x_{\sigma^{-1}\sigma n})=g(x_1,\cdots,x_n)\end{aligned}$$

so θ_σ is injective. Now, for any $f(x_1,\cdots,x_n)$, we have

$$\theta_\sigma\left[f(x_{\sigma^{-1}1},\cdots,x_{\sigma^{-1}n})\right]=f(x_1,\cdots,x_n)$$

so θ_σ is surjective. Thus, θ_σ is a bijective ring homomorphism from $R[x_1,\cdots,x_n]$ to itself, so it is a ring automorphism. □

(b) Show that $\sigma\mapsto\theta_\sigma$ is a group homomorphism $S_n\to\operatorname{aut}R[x_1,\cdots,x_n]$, which is injective.

Proof. Let $\sigma,\tau\in S_n$. Then consider $\theta_{\sigma\tau}$. For some $f(x_1,\cdots,x_n)\in R[x_1,\cdots,x_n]$, we have

$$\begin{aligned}\theta_{\sigma\tau}\left[f(x_1,\cdots,x_n)\right]&=f(x_{\sigma\tau 1},\cdots,x_{\sigma\tau n})\\&=\theta_\sigma\left[f(x_{\tau 1},\cdots,x_{\tau n})\right]\\&=\theta_\sigma(\theta_\tau\left[f(x_1,\cdots,x_n)\right])\\&=(\theta_\sigma\circ\theta_\tau)\left[f(x_1,\cdots,x_n)\right]\end{aligned}$$

so $(\sigma\tau)\mapsto\theta_{\sigma\tau}=\theta_\sigma\circ\theta_\tau$ and this is indeed a group homomorphism. Now consider the kernel of this homomorphism. The identity in $\operatorname{aut}R[x_1,\cdots,x_n]$ is the identity map, which is

$$\theta_\varepsilon\left[f(x_1,\cdots,x_n)\right]=f(x_1,\cdots,x_n)$$

So the kernel only contains the identity permutation, ε. Thus, we have $S_n/\{\varepsilon\}\cong S_n$ which is isomorphic to the image of this homomorphism, so it is indeed injective. □

(c) If $G\subseteq\operatorname{aut}R[x_1,\cdots,x_n]$ is a subgroup, show that $S_G=\{\,f\mid\theta(f)=f,\forall\theta\in G\,\}$ is a subring of $R[x_1,\cdots,x_n]$.

Proof. Clearly $1\in S_G$ since all automorphisms must fix 1. Now if $f,g\in S_G$, then.

$$\begin{aligned}\theta(f+g)=\theta(f)+\theta(g)=f+g\\\theta(f\cdot g)=\theta(f)\cdot\theta(g)=f\cdot g\end{aligned}$$

so $f+g,fg\in S_G$, and thus S_G is indeed a subring of $R[x_1,\cdots,x_n]$. □