Homework 7

Aleck Zhao

March 30, 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.

Section 6.4: Finite Fields

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

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 $f \not\cong 0$ in $F[x]$.
    (b) If $\operatorname{char} F = 0$, show that 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)

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 $f(u+a), a \in \mathbb{F}_p)$ tin

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.)
    (b) Show that the degree of each monic irreducible divisor f of $x^{p^n} - x$ is a divisor of n. (Hint: Theorem 5)
    (c) Factor $x^8 - x$ into irreducibles in $\mathbb{F}_2[x]$.

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 $\theta_\sigma [f(x_1, \cdots, x_n)] = f(x_{\sigma 1}, \cdots, x_{\sigma n})$.

(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 $f, g \in R[x_1, \cdots, x_n]$,

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

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,

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

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

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

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

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

so $(\sigma\tau) \mapsto \theta_{\sigma\tau} = \theta_\sigma \circ \theta_\tau$ and this is indeed a group homomorphism. Suppose $\theta_\sigma = \theta_\tau$ for some $\sigma, \tau \in S_n$. □

¡++¿

(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 $R[x_1, \cdots, x_n]$.