**Honors Algebra** **Spring 2025**
**HW 6: Fields** **3/18/2025**

*Abstract Algebra: An Integrated Approach by J.H. Silverman.*
Page 180-186: 7.14, 7.22, 7.29
Page 214-220: 8.3, 8.8, 8.21, 8.23
Page 320-325: 10.6, 10.12
Page 357-370: 11.2, 11.7, 11.8

**Problem 1** (7.14). Let $R$ be a commutative ring.

(a) Suppose that $a, b \in R$ have the property that $aR + bR = R$. Prove that for all $m, n \geq 1$ we have

$$a^m R + b^n R = R$$

(b) More generally, let $a_1, \ldots, a_t \in R$, and let $e_1, \ldots, e_t \geq 1$ be positive integers. Prove that

$$a_1 R + a_2 R + \cdots + a_t R = R \iff a_1^{e_1} R + a_2^{e_2} R + \cdots + a_t^{e_t} R = R$$

**Problem 2** (7.22). Let $R$ be a ring, let $P \subset R$ be a prime ideal, let $S = R\ P$ be the complement of $P$, let $R_S$ be the localization ring as described in Exercise 7.21, and let

$$Q = \{(a, b) \in R_S : a \in P\}$$

Prove that $Q$ is the unique maximal ideal of $R_S$. (A ring with a unique maximal ideal is called a local ring; see Exercise 3.53).

**Problem 3** (7.29). A polynomial $f(X_1, \ldots, X_n) \in F[X_1, \ldots, X_n]$ is said to be homogeneous of degree k if

$$f(aX_1, \ldots, aX_n) = a^k f(X_1, \ldots, X_n) \text{ for all } a \in F$$

(a) Prove that $f$ is a homogeneous polynomial of degree $k$ if and only if $f$ is a sum of the form

$$f(X_1, \ldots, X_n) = \sum_{\substack{i_1, i_2, \ldots, i_n \geq 0 \\ i_1 + i_2 + \cdots + i_n = k}} c_{i_1, i_2, \ldots, i_n} X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}$$

(b) Prove that the elementary symmetric polynomials $s_k(X_1, \ldots, X_n)$ described in Definition 7.40 is a homogeneous polynomial of degree $k$.

(c) Let $f(X_1,\ldots,X_n) \in F(X_1,\ldots,X_n)$ be homogeneous of degree $k$. Prove that

$$X_1\frac{\partial f}{X_1} + X_2\frac{\partial f}{X_2} + \cdots + X_n\frac{\partial f}{X_n} = kf$$

(*Hint.* If you view

$$f(TX_1,\ldots,TX_n) = T^k f(X_1,\ldots,X_n)$$

as being a relation in the polynomial ring $F[T,X_1,\ldots,X_n]$, then you can differentiate it with respect to $T$. Then set $T=1$.)

**Problem 4** (8.3)**.** This exercise sketches a proof of the following result, which says that if a number is the root of a polynomial in $Q[x]$, then it cannot be too closely approximated by rational numbers.

**Theorem 8.46** Let $f(x) \in Q[x]$ be a polynomial ofdegree $d \geq 1$. There is a positive constant $C_f > 0$ such that if $\alpha \in mathbbC\ \mathbb{Q}$ is a non-rational root of $f(x)$, then

$$\left|\frac{p}{q} - \alpha\right| \geq \frac{C_f}{q^d} \text{ for all } \frac{p}{q} \in \mathbb{Q}$$

(a) Prove that every $p/q \in mathbbQ$ satisfies either

$$f\left(\frac{p}{q}\right) = 0 \text{ or } \left|f\left(\frac{p}{q}\right)\right| \geq \frac{1}{q^d}$$

(b) Let $g(x) \in \mathbb{C}[x]$ be a polynomial of degree $e$, and let $\alpha \in \mathbb{C}$. Prove that there is a constant $A_{g,\alpha}$ so that

$$|g(\beta)| \leq A_{g,\alpha}\max\{1, |\beta-\alpha|^e\} \ \ \beta \in \mathbb{C}$$

(*Hint.* Expand $g(x)$ as a sum of powers of $x-\alpha$)

(c) Use (a) and (b) to prove Theorem 8.46. (*Hint.* Since we are given that $f(\alpha) = 0$), we can factor $f(x)$ as $f(x) = (x-\alpha)g(x)$ for some $g(x) \in \mathbb{C}[x]$.)

**Problem 5** (8.8)**.** Let $F$ be a finite field of order $q$, and assume that $q$ is odd.

(a) Let $a, b \in F*$. If $a^2 = b^2$, prove that either $a = b$ or $a = -b$.

(b) Show by way of an example that (a) is not true for the rings $\mathbb{Z}/8\mathbb{Z}$ and $\mathbb{Z}/15\mathbb{Z}$.

(c) Let

$$\mathcal{R} = \{a^2 : a \in F*\} \text{ and } \mathcal{N} = \{b \in F* : b \notin \mathcal{R}\}$$

be, respectively, the set of squares and non-squares in $F*$. Prove that $\mathcal{R}$ and $\mathcal{N}$ each contain exactly $(q-1)/2$ distinct elements.

(d) Let $f(x)$ be the polynomial

$$f(x) = x^{\frac{q-1}{2}} - 1$$

Prove that $\mathcal{R}$ is exactly the set of roots of $f(x)$ in $F$. (*Hint.* Use Lagrange to prove that the elements of $\mathcal{R}$ are roots. Then use (c) and Theorem 8.8(c).)

(e) Let $c \in F*$. Prove that

$$c^{\frac{q-1}{2}} \equiv \begin{cases} 1 & \text{if } c \in \mathcal{Q} \\ -1 & \text{if } c \in \mathcal{N} \end{cases}$$

(*Hint.* Lagrange says that every element of $F*$ is a root of $x^{q-1} - 1$. Factor this polynomial as $f(x)g(x)$ and use (d).)

(f) Let $a_1, a_2 \in \mathcal{R}$ and $b_1, b_2 \in \mathcal{N}$. Prove that

$$a_1 a_2 \in \mathcal{R} \text{ and } b_1 b_2 \in \mathcal{R}$$

The first of these facts is hardly surprising, since indeed, the product of two squares is a square in any commutative ring. But the second fact is surprising, since in most rings, most products of non-square won't be squares.

**Problem 6** (8.21)**.** Let $\Phi_1(x) = x - 1$, and for $n/geq1$, define the $n$th cyclotomic polynomial $\Phi_n(x)$ inductively by the formula

$$x^n - 1 = \prod_{m|n} \Phi_m(x)$$

as described in Definition 8.37.

(a) Compute $\Phi_n(x)$ for all $2 \leq n \leq 10$.

(b) Let $\zeta_n = e^{2\pi i/n} \in \mathbb{C}$ be a primitive $n$th-root of unity. Prove that $\Phi_n(x)$ factors in $\mathbb{C}[x]$ as

$$\Phi_n(x) = \prod_{\substack{1 \leq d \leq d \\ \gcd(d,n)=1}} (x - \zeta_n^d)$$

Thus $\Phi_n(x)$ is a monic polynomial in $\mathbb{C}[x]$.

(c) Prove that all the coefficients of $\Phi_n(x)$ are in $\mathbb{Z}$.

**Problem 7** (8.23)**.** Let $R$ be a PID with fraction field $K$, let $\pi \in R$ be an irreducible element, and let

$$f(x) = c_0 = c_1 x + \cdots + c_d x^d \in R[x]$$

be a polynomial whose coefficients satisfy

$$\pi \nmid c_d, \quad \pi | c_i \text{ for } 0 \leq i < d, \quad \text{ and } \pi^2 \nmid c_0$$

Prove that $f(x)$ is irreducible in $K[x]$.

**Problem 8** (10.6)**.** Let $V$ be the $\mathbb{R}$-vector space of polynomials of degree at most 3,

$$V = \{a + bx + cx^2 + dx^3 : a, b, c, d \in \mathbb{R}\}$$

(a) Prove that the following sets are $\mathbb{R}$-bases for $L$:

$$\text{(i) } \mathcal{A} = \{1, x, x^2, x^3\} \qquad \text{(ii) } \mathcal{B} = \{1, x+1, (x+1)^2, (x+1)^3\}$$

(b) Let $L : V \longrightarrow V$ be differentiation: i.e.,

$$L : V \longrightarrow V, \quad L(a + bx + cx^2 + dx^3) = b + 2cx + 3dx^2$$

Using the bases in (a), compute the following matrices associated to $L$:

$$\text{(i) } \mathcal{M}_{L,\mathcal{A},\mathcal{A}} \qquad \text{(ii) } \mathcal{M}_{L,\mathcal{B},\mathcal{A}}$$

**Problem 9** (10.12)**.** Let $V$ be a finite-dimensional vector space, and let $L \in \mathrm{End}_F(V)$. Prove that the following are equivalent:

(a) There is an $L_1 \in \mathrm{End}_F(V)$ satisfying $LL_1 = I$. (We say that $L_1$ is a right-inverse)

(b) There is an $L_2 \in \mathrm{End}_F(V)$ satisfying $L_2L = I$. (We say that $L_2$ is a left-inverse)

N.B. Be sure that you use the hypothesis that $V$ is finite dimensional, since the statement is false for infinite-dimensional vector spaces.

**Problem 10** (11.2)**.** Let $R$ be a ring, and let $a_1, \ldots, a_n \in R$. We define an evaluation map

$$E_a : R[x] \longrightarrow R^n, \quad E_a(f(x)) = (f(a_1), \ldots, f(a_n))$$

(a) Prove that $E_a$ is an $R$-module homomorphism

(b) Suppose that $R$ is an integral domain. Prove that the kernel of $E_a$ is a principal ideal of $R[x]$. Find a generator for this ideal.

(c) Is (b) true if we drop the assumption that $R$ is an intergral domain?

**Problem 11** (11.7)**.** THis exercise asks you to generalize Propostiion 11.18. Let $M$ be an $R$-module. For each ideal $I$ of $R$, we define $IM$ to be the set

$$IM = \{a_1m_1 + \cdots + a_km_k : k \geq 0, a_1, \ldots, a_k \in I, m_1, \ldots, m_k \in M\}$$

(a) Prove that $IM$ is a submodule of $M$.

(b) Prove that the quotient module $M/IM$ has a natural structure as an $R/I$-module.

(c) More generally, let $J \subseteq I$ be ideals of $R$, and let $K$ be the set

$$K = \{r \in R : rI \subseteq J\}$$

Prove that $K$ is an ideal of $R$, that $JM$ is a submodule of $IM$, and that the quotient $IM/JM$ is naturally an $R/K$-module.

(d) Suppose that $R$ is an integral domain, and suppose that the ideals $I$ and $J$ in (c) are principal, say $I = aR$ and $J = bR$. Prove that $b = ac$ for some $c \in R$ and that the ideal $K$ defined in (c) is the principal ideal $cR$.

**Problem 12** (11.8)**.** Let $M$ be a finitely generated free $R$-module, and let $J$ be a maximal ideal of $R$. Prove that

$$\mathrm{rank}_R(M) = \dim_{R/J}(M/JM)$$

Explain why this equality gives an alternative proof of Theorem 11.27; i.e., explain why it implies that every basis of $M$ has the same number of elements. (See Exerecise 11.7 for the definition of the submodule $JM$)