Math 562/662 **Spring 2019**
Homework 3 **Drew Armstrong**

---

1. The Definition of PIDs is Good. For any ring R prove that

$$(R \text{ is a field}) \iff (R[x] \text{ is a PID}).$$

2. Quadratic Field Extensions, Part II. Let $\mathbb{E} = \mathbb{F}(\iota) \supseteq \mathbb{F}$ for some element $\iota \in \mathbb{E}$ satisfying $\iota \notin \mathbb{F}$ and $\iota^2 \in \mathbb{F}$. Recall that the vector space $\mathbb{E}/\mathbb{F}$ has basis $\{1, \iota\}$ and the Galois group $\text{Gal}(\mathbb{E}/\mathbb{F})$ is generated by the "conjugation" automorphism $(a + b\iota)^* := a - b\iota$.

(a) For any $\alpha \in \mathbb{E}$ show that $\alpha \in \mathbb{F}$ if and only if $\alpha^* = \alpha$. Use this to show that $\alpha\alpha^*$ and $\alpha + \alpha^*$ are in $\mathbb{F}$ for all $\alpha \in \mathbb{E}$.

(b) For any polynomial $f(x) = \sum_i \alpha_i x^i \in \mathbb{E}[x]$ we define $f^*(x) := \sum_i \alpha_i^* x^i$. Show that this is a ring automorphism $* : \mathbb{E}[x] \to \mathbb{E}[x]$. Use this to prove that $f(x)f^*(x)$ and $f(x) + f^*(x)$ are in $\mathbb{F}[x]$ for all $f(x) \in \mathbb{E}[x]$.

(c) For all $f(x) \in \mathbb{F}[x]$ show that the roots of $f(x)$ in $\mathbb{E} - \mathbb{F}$ come in conjugate pairs.

(d) **Application.** Let $f(x) \in \mathbb{F}[x]$ have degree 3. If f has a root in $\mathbb{E}$, prove that f also has a root in $\mathbb{F}$. [Hint: Use Descartes' Factor Theorem.]

3. Wilson's Theorem. We saw in the previous problem that any ring homomorphism $\varphi : R \to S$ extends to a ring homomorphism $\varphi : R[x] \to S[x]$ by acting on coefficients. Now let $p \in \mathbb{Z}$ be prime and consider the following polynomial with integer coefficients:

$$f(x) := x^{p-1} - 1 - \prod_{k=1}^{p-1}(x - k) \in \mathbb{Z}[x].$$

(a) Let $\pi : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ be the quotient homomorphism. Prove that the polynomial $f^\pi(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ has $p - 1$ distinct roots and degree $< p - 1$. [Hint: Fermat's Little Theorem.]

(b) Use Descartes' Factor Theorem to show that every coefficient of $f(x) \in \mathbb{Z}[x]$ is a multiple of p. Show that this implies $(p - 1)! = -1 \bmod p$.

4. Gaussian Integers (Optional). The following theorem is due to Fermat:

> An integer $n \in \mathbb{N}$ is a sum of two squares if and only if any prime factor $p|n$ satisfying $p = 3 \bmod 4$ occurs to an even power.

In this problem we will give an algebraic proof due to Gauss. Let $i \in \mathbb{C}$ be a fixed square root of -1 and consider the following ring extension of $\mathbb{Z}$, called the ring of *Gaussian integers*:

$$\mathbb{Z} \subseteq \mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}.$$

(a) Let $N : \mathbb{Z}[i] \to \mathbb{N}$ be the "norm" function defined by $N(a + ib) := a^2 + b^2$. Prove that $(\mathbb{Z}[i], N)$ is a Euclidean domain, hence $\mathbb{Z}[i]$ is a UFD. [Hint: For any $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$, the ideal $\beta\mathbb{Z}[i]$ is the set of vertices of a square grid in $\mathbb{C}$ with (squared) side length $N(\beta)$. Let $\beta\zeta$ be the closest element of $\beta\mathbb{Z}[i]$ to α and observe that $N(\alpha - \beta\zeta) < N(\beta)$.]

(b) For all $\alpha, \beta \in \mathbb{Z}[i]$ prove that $N(\alpha\beta) = N(\alpha)N(\beta)$. Use this to show that

$$\mathbb{Z}[i]^\times = \{\alpha \in \mathbb{Z}[i] : N(\alpha) = 1\} = \{\pm 1, \pm i\}.$$

(c) For all $n \in \mathbb{N}$ show that $n = 3 \bmod 4$ implies $n \notin \text{im}\, N$. [Hint: What are the square elements of the ring $\mathbb{Z}/4\mathbb{Z}$?]

(d) Use induction on n to prove the following statement:

$$n \in \operatorname{im} N \Rightarrow (\text{every prime } p|n \text{ with } p = 3 \bmod 4 \text{ occurs to an even power}).$$

[Hint: Let $n = a^2 + b^2 \in \operatorname{im} N$ and let $p \in \mathbb{Z}$ be prime. If $p = 3 \bmod 4$ use (b) and (c) to show that p is irreducible in $\mathbb{Z}[i]$. Then if $p|n$ use (a) to show that $p|(a+bi)$ or $p|(a-bi)$ in $\mathbb{Z}[i]$. In either case show that $p|a$ and $p|b$, hence $n/p^2 \in \operatorname{im} N$.]

(e) Conversely, for prime $p \in \mathbb{N}$ show that $p = 1 \bmod 4$ implies $p \in \operatorname{im} N$. [Hint: Let $p = 4k+1$ and assume for contradiction that $p \notin \operatorname{im} N$. Use (a) and (b) to show that p is irreducible and hence prime in $\mathbb{Z}[i]$. On the other hand, set $m := (2k)!$ and use Wilson's Theorem to show that $p|(m-i)(m+i)$.]

(f) Finish the proof.

5. $\mathbb{Z}[\sqrt{-3}]$ is not a UFD. Let $\sqrt{-3} \in \mathbb{C}$ be a fixed square root of -3 and consider the ring

$$\mathbb{Z} \subseteq \mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}.$$

(a) Let $N : \mathbb{Z}[\sqrt{-3}] \to \mathbb{N}$ be defined by $N(a + b\sqrt{-3}) := a^2 + 3b^2$. For all $\alpha, \beta \in \mathbb{Z}[\sqrt{-3}]$ prove that $N(\alpha\beta) = N(\alpha)N(\beta)$ and use this to show that

$$\mathbb{Z}[\sqrt{-3}]^\times = \{\alpha \in \mathbb{Z}[\sqrt{-3}] : N(\alpha) = 1\} = \{\pm 1\}.$$

(b) Prove that there is no element $\alpha \in \mathbb{Z}[\sqrt{-3}]$ with $N(\alpha) = 2$. Use this to show that any element with $N(\alpha) = 4$ is irreducible. In particular, $2 \in \mathbb{Z}[\sqrt{-3}]$ is irreducible.

(c) But show that $2 \in \mathbb{Z}[\sqrt{-3}]$ is **not prime** because

$$2|(1+\sqrt{-3})(1-\sqrt{-3}) \text{ and } 2 \nmid (1+\sqrt{-3}) \text{ and } 2 \nmid (1-\sqrt{-3}).$$

(d) Use this to prove that the following ideal is **not principal**:

$$\{2\alpha + (1+\sqrt{-3})\beta : \alpha, \beta \in \mathbb{Z}[\sqrt{-3}]\} \subseteq \mathbb{Z}[\sqrt{-3}].$$

6. Field of Fractions. In this problem you will show that "integral domain" and "subring of a field" are the same concept. Let R be an integral domain and consider the following set of abstract symbols, called *fractions*:

$$\operatorname{Frac}(R) := \left\{ \frac{a}{b} : a, b \in R, b \neq 0 \right\}.$$

(a) Prove that the following relation is an equivalence on the set of fractions:

$$\frac{a}{b} \sim \frac{a'}{b'} \quad \iff \quad ab' = a'b.$$

(b) Prove that the following operations are well-defined on equivalence classes:

$$\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd} \qquad \text{and} \qquad \frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd}.$$

It follows that the set of equivalence classes $\operatorname{Frac}(R)/\sim$ is a field. Following tradition, we will just call it $\operatorname{Frac}(R)$ and we will write $=$ instead of $\sim$. Furthermore, we will write $R \subseteq \operatorname{Frac}(R)$ for the image of the injective ring homomorphism $a \mapsto a/1$.

(c) **Universal Property.** Let $\mathbb{F}$ be a field and let $\varphi : R \to \mathbb{F}$ be any ring homomorphism. Prove that this extends to a unique ring homomorphism $\varphi : \operatorname{Frac}(R) \to \mathbb{F}$, which is injective if and only if φ is. [Hint: Show that $\varphi(a/b) := \varphi(a)/\varphi(b)$ is well-defined.]

7. Newton's Theorem on Symmetric Polynomials. Given a ring R and a set of "independent variables" $\mathbf{x} = \{x_1, \ldots, x_n\}$ we define *multivariate polynomials* by induction:

$$R[\mathbf{x}] = R[x_1, \ldots, x_n] := R[x_1, \ldots, x_{n-1}][x_n] = \left\{ f(\mathbf{x}) = \sum_{\mathbf{k} \in \mathbb{N}^n} a_{\mathbf{k}} \mathbf{x}^{\mathbf{k}} : a_{\mathbf{k}} \in R \right\}.$$

To save space we use the notations $\mathbf{k} = (k_1, \ldots, k_n) \in \mathbb{N}^k$ and $\mathbf{x}^{\mathbf{k}} = x_1^{k_1} \cdots x_n^{k_n}$. We assume that all but finitely many of the coefficients $a_{\mathbf{k}} \in R$ are zero.

(a) We say that a polynomial $f(\mathbf{x}) = R[\mathbf{x}]$ is *symmetric* if for all $\sigma \in S_n$ we have

$$f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = f(x_1, \ldots, x_n).$$

Observe that the symmetric polynomials are a subring of $R[\mathbf{x}]$.

(b) **Newton's Theorem.** Recall the definition of the *elementary symmetric polynomials*:

$$e_k(x_1, \ldots, x_n) := \sum_{1 \leq i_1 < \cdots < i_k \leq n} x_{i_1} \cdots x_{i_k}.$$

For convenience, let's define $\mathbf{e}^{\mathbf{k}} := e_1^{k_1} \cdots e_n^{k_n}$. For any symmetric polynomial $f(\mathbf{x}) = \sum_{\mathbf{k}} a_{\mathbf{k}} \mathbf{x}^{\mathbf{k}} \in R[\mathbf{x}]$, prove that there exist some $b_{\mathbf{k}} \in R$ such that $f(x) = \sum_{\mathbf{k}} b_{\mathbf{k}} \mathbf{e}^{\mathbf{k}}$. [Hint: Order the degree vectors $\mathbf{k} \in \mathbb{N}^n$ by "dictionary order" and let $a_{\mathbf{k}} \mathbf{x}^{\mathbf{k}}$ be the "leading term." By symmetry of f we must have $k_1 \geq k_2 \geq \cdots \geq k_n$. Show that there exists $\mathbf{k}' \in \mathbb{N}^k$ so that $a_{\mathbf{k}} \mathbf{e}^{\mathbf{k}'}$ has the same leading term, hence $f(\mathbf{x}) - a_{\mathbf{k}} \mathbf{e}^{\mathbf{k}'}$ is a symmetric polynomial of "smaller degree."]

(c) **Important Corollary.** Suppose that a polynomial $f(x) \in R[x]$ of degree n splits in some ring extension $E \supseteq R$. That is, suppose that we have

$$f(x) = x^n - e_1 x^{n-1} + e_2 x^{n-2} - \cdots + (-1)^n e_n = (x - \alpha_1) \cdots (x - \alpha_n) \in E[x].$$

Prove that any "symmetric expression of the roots" is in R.

(d) **Application: Discriminant of a Cubic.** Let $f(x) = x^3 + ax^2 + bx + c \in R[x]$ and let $E \supseteq R$ be a ring extension such that

$$x^3 + ax^2 + bx + c = (x - \alpha)(x - \beta)(x - \gamma) \in E[x].$$

From part (c) we know that the following element of E (called the *discriminant* of f) is actually in R:

$$\mathrm{Disc}(f) := (\alpha - \beta)^2 (\alpha - \gamma)^2 (\beta - \gamma)^2.$$

Use the algorithm from part (b) to express $\mathrm{Disc}(f)$ as a specific polynomial in the coefficients. [I'll get you started: Note that $\mathrm{Disc}(f) = (\alpha^4\beta^2 + \text{lower terms})$ and $a^2b^2 = (\alpha^4\beta^2 + \text{lower terms})$. Now find the leading term of $\mathrm{Disc}(f) - a^2b^2$.]