NOTE: To give you more flexibility as you split your time between this problem set and the project: the score that will count in your grade will be 1.25 times your original score, up to a maximum of 100% of the original points. Therefore any score above 80% of the possible points will be counted as 100%.

- **Read:** §19 (through Example 4 on page 198), §20.

1. Let $K = \{a + b\sqrt{2} : \ a, b \in \mathbb{Q}\}$. It was shown in PSet 8 problem 3 that K is a field. In this problem, we will study the automorphisms of K (an automorphism is a bijective homomorphism from K to itself).

   (a) Suppose that $\phi : K \to K$ is an automorphism. Prove that $\phi(1) = 1$. (This requires only a one-sentence argument if you cite an appropriate theorem from the text).

   (b) Suppose that ϕ is an automorphism. Prove that $\phi(\sqrt{2})$ must be either $\sqrt{2}$ or $-\sqrt{2}$.
   Hint: Use properties of homomorphisms, and part (a), to find an equation that $\phi(\sqrt{2})$ must satisfy.

   (c) Use (a) and (b) to prove that there are exactly two automorphisms of K.

   Comment: The automorphisms of a field extension $K \supseteq \mathbb{Q}$ form a group called the *Galois group* of the field. In this case, the Galois group is isomorphic to $\mathbb{Z}_2$ Galois groups are the basis of a beautiful and deep theory linking field extensions to groups, called *Galois Theory.*

2. (a) Let I and J be ideals in a ring R, such that $I + J = R$. Prove that

   $$R/(I \cap J) \cong (R/I) \oplus (R/J).$$

   Hint: Apply the fundamental theorem of ring homomorphisms. Ask for a further hint if you get stuck.

   (b) Deduce from (a) and a problem on an earlier problem set that if m an n are relatively prime integers, then

   $$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}.$$

   This fact is sometimes called the "Chinese remainder theorem."

3. Let F be a field.

   (a) Determine the unit group $F[X]^\times$ of the polynomial ring $F[X]$.

   (b) Show that if $c \in F$, $c \neq 0_F$, then for every $f(X) \in F[X]$, the elements $f(X)$ and $cf(X)$ generate the same principal ideal in $F[X]$.
   (See Example 12 on p. 170 for the terminology. Note that in §20 we'll use the more succinct notation $(f(X))$ to denote the principal ideal generated by $f(X)$, instead of the more cumbersome $F[X] \cdot f(X)$).

4. Let K be a field, and R be a ring that contains K as a subring ($K \subseteq R$), and let $r \in R$ be any element of R. Define a function $\phi_r : \ K[X] \to R$ by the formula $\phi_r(f(X)) = f(r)$.

   (a) Prove that ϕ_r is a ring homomorphism (it is called an *evaluation homomorphism*).

   (b) Prove that if ϕ_r is surjective, then the ring R is isomorphic to some quotient of the polynomial ring $K[X]$.

Note: The remaining problems are most easily solved using topics we will cover over the course of the week. All of them should be tractible using tools we cover by Wednesday's class.

5. Consider the evaluation homomorphism $\phi_i : \mathbb{R}[X] \to \mathbb{C}$ given by $\phi_i(f(X)) = f(i)$. Prove that, as we claimed in class, the kernel of this homomorphism is the principal ideal generated by $X^2 + 1$.

6. Write each polynomial as a product of irreducible polynomials in the specified polynomial ring (this is exercise 19.3 in Saracino; you can check your answer to two of these in the back of the book).

   (a) $2X^3 + X^2 + 2 \in \mathbb{Z}_3[X]$
   (b) $X^3 + 3X^2 + X + 4 \in \mathbb{Z}_5[X]$
   (c) $X^2 + 5 \in \mathbb{Z}_7[X]$
   (d) $X^4 + X^3 + 2X^2 + X + 2 \in \mathbb{Z}_3[X]$
   (e) $X^5 + X^2 - X - 1 \in \mathbb{Z}_2[X]$

7. Let p be a prime number.

   (a) Prove that the quotient ring $\mathbb{Z}_p[X]/(X^2 + 1)$ is a field if and only if there are no integer solutions to the congruence $x^2 \equiv -1 \pmod{p}$.
   (b) Suppose that $\mathbb{Z}_p[X]/(X^2 + 1)$ is a field. How many element are in this field? (Express your answer in terms of p.)