Math 476 - Abstract Algebra 1
Day 30 Group Assignment **Name:**_____

1. You may present portions of Activity 9.7 on page 109 in your textbook. However, you must present (a), (b), and (c) at the same time, the same goes for (d) and (e); (f) and (g); (h) and (i); and (j) and (k).

   Definition: Let F be a field.

   - A **subfield** of F is a subring of F that is also a field.
   - If F is a subfield of another field E, then E is said to be a **field extension** (or simply an **extension**) of F.
   - If E is an extension of F and S is a subset of E, then the set $F(S)$, called the extension of F **generated by** S, is defined to be the smallest subfield of E that contains all of the elements of both F and S. In the case where S contains a single element $\alpha \in E$, then $F(\alpha)$ is called a **simple extension**.

2. Consider the set $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.

   (a) Prove that $\mathbb{Q}(\sqrt{2})$ is a *subring* of $\mathbb{R}$.

   (b) Prove that $\mathbb{Q}(\sqrt{2})$ is a *subfield* of $\mathbb{R}$.

Theorem 9.10 Let F be a field, and let $p(x)$ be a quadratic polynomial with coefficients from F sich that $p(x)$ has no roots in F. Suppose also that $p(x)$ does have a root α in some extension E or F. Then the simple extension of F generated by α (that is, the smallest field containing both F and α) can be described as follows: $F(\alpha) = \{u + v\alpha : u, v \in F\}$.

Proof: Let $p(x) = ax^2 + bx + c$ for some $a, b, c \in F$. WLOG, we may assume that $a = 1$, so that $p(x) = x^2 + bx + c$. Since α is a root of $p(x)$, it follows that $\alpha^2 + b\alpha + c = 0$, or equivalently, $\alpha^2 = -b\alpha - c$.

to complete the proof, we must show that the set $S = \{u + v\alpha : u, v \in F\}$ is the smallest subfield of E that contains both α and the elements of F. We will first show that S is a subfield of E. We will do so by showing that S is a subring of E and that S is a field. By definition, S is non-empty.

Let $u + v\alpha$ and $w + z\alpha$ be elements of S. Then $(u + v\alpha) - (u + z\alpha) = (u - w) + (v - z)\alpha$, which is an element of S, so S is closed under subtraction.

Similarly, $(u+v\alpha)(u+z\alpha) = uw+vw\alpha+uz\alpha+vz\alpha^2 = uw+vw\alpha+uz\alpha+vz(-b\alpha-c) = uw+vw\alpha+uz\alpha-vzb\alpha-vzc = (uw - vzc) + (vw + uz - vzb)\alpha$, which is an element of S. Thus S is a subring of E.

Since E is a field, S inherits commutativity from E. Also, if we take $u = 1$ and $v = 0$, then $1 \in S$. All that remains is to show that every non-zero element of S is a unit. That is, for every element $(u + v\alpha)$ with u and v not both zero, we must find an element $w + z\alpha$ such that $(u + v\alpha)(u + z\alpha) = 1$. We claim that the required element is $w = (-u + vb)\beta^{-1}$ and $z = v\beta^{-1}$ where $\beta = -u^2 + buv - cv^2$, where β^{-1} is the multiplicative inverse of β in F. See the derivation on p. 112 of your book for the computational details.

Finally, we must argue that S is the smallest subfield of E that contains both α and all of the elements of F. To see this, notice that if K is a field that contains both α and F, then K must also contain $u + v\alpha$ for all $u, v \in F$. Thus S is a subfield of K. $\square$.

3. Explain why, at the beginning of the proof of Theorem 9.10, it was ok for us to assume that $a = 1$.

4. Explain in more detail, why, at the end of the proof, we are able to argue that if K is a field that contains both α and F, then K must also contain $u + v\alpha$ for all $u, v \in F$.

Theorem 9.12:(Kronecker's Theorem). Let F be a field, and let $p(x)$ be a non-constant polynomial with coefficients from F. Then there exists an extension E of F and an element $\alpha \in E$ such that $p(\alpha) = 0$.

Definition 9.14: Let R and S be rings. The **Cartesian Product** of R and S is the set $R \times S = \{(r, s) : r \in R, s \in S\}$. The **direct sum** of R and S, denoted $R \oplus S$, is the set $R \times S$ with addition and multiplication defined componentwise. That is,

$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$ and $(r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2)$.

Theorem 9.15: Let R and S be rings. Then $R \oplus S$ is also a ring.

Note: You may prove each of the necessary axioms as presentation problems (with the exception of the one that is proved in your textbook).

Theorem 9.16: Let R and S be rings. Then $R \oplus \{0_S\} = \{(r, 0_S) : r \in R\}$ and $\{0_R\} \oplus S = \{(0_R, s) : s \in S\}$ are both subrings of $R \oplus S$.

5. Make addition and multiplication tables for the ring $\mathbb{Z}_3 \oplus \mathbb{Z}_2$. Then, find $char(\mathbb{Z}_3 \oplus \mathbb{Z}_2)$.