HOMEWORK #9, DUE THURSDAY APRIL 25TH

1. Herstein, Chapter 4, §4, 2: Let R be the Gaussian integers and let M be the subset of Gaussian integers $a + bi$ such that a and b are divisible by 3. Show that M is an ideal and the quotient R/M is a field with 9 elements.
2. Herstein, Chapter 4, §4, 3: (i) Let
$$R = \{\, a + b\sqrt{2} \mid a,\, b \text{ integers} \,\}.$$
Show that R is a subring of the complex numbers.
(ii) Let
$$M = \{\, a + b\sqrt{2} \in R \mid a,\, b \text{ are divisible by } 5 \,\}.$$
Show that M is an ideal and the quotient R/M is a field with 25 elements. (*Hint*: consider the identity $a^2 - 2b^2 = (a+b\sqrt{2})(a-b\sqrt{2})$.)
3. Construct a field with 49 elements.
4. Let R be a ring and let I be an ideal of R, not equal to R. Suppose that every element not in I is a unit. Prove that I is the unique maximal ideal in R.
5. Let $\phi\colon R \longrightarrow S$ be a ring homomorphism and suppose that J is a prime ideal of S.
(i) Prove that $I = \phi^{-1}(J)$ is a prime ideal of R.
(ii) Give an example of an ideal J that is maximal such that I is not maximal.
6. Let R be an integral domain and let a and b be two elements of R. Prove that:
(i) $a|b$ if and only if $\langle b \rangle \subset \langle a \rangle$.
(ii) a and b are associates if and only if $\langle a \rangle = \langle b \rangle$.
(iii) Show that a is a unit if and only if $\langle a \rangle = R$.
7. Prove that every prime element of an integral domain is irreducible.
8. Let R be an integral domain. Let a and b be two elements of R. Show that if d and d' are both a gcd for the pair a and b, then d and d' are associates.
9. (i) Show that the elements 2, 3 and $1 \pm \sqrt{-5}$ are irreducible elements of
$$R = \mathbb{Z}[\sqrt{-5}] = \{\, a + b\sqrt{-5} \mid a, b \in \mathbb{Z} \,\}.$$
(ii) Show that every element of R can be factored into irreducibles.
(iii) Show that R is not a UFD.
10. Let R be a UFD.

(i) Prove that for every pair of elements a and b of R, we may find an element $m = [a, b]$ that is a **least common multiple**, that is,

(1) $a|m$ and $b|m$, and
(2) if $a|m'$ and $b|m'$ then $m|m'$.

Show that any two lcm's are associates.
(ii) Show that if (a, b) denotes the gcd then $(a, b)[a, b]$ is an associate of ab.
Challenge Problem: 11. Let S be a commutative semigroup, that is, a set together with a binary operation that is associative, commutative, and for which there is an identity, but not necessarily inverses. Treating this operation like multiplication in a ring, define what it means for S to have unique factorisation.
Challenge Problem: 12. Let $v_1, v_2, \dots, v_n$ be a sequence of elements of $\mathbb{Z}^2 = \mathbb{Z} \oplus \mathbb{Z}$. Let S be the semigroup that consists of all linear combinations of $v_1, v_2, \dots, v_n$, with non-negative integral coefficients. Let the binary rule be ordinary addition. Determine which semigroups have unique factorisation.