Homework 11, due on Friday, November 20

Read carefully chapters 20, 21, 22 in the textbook and the notes posted on the course web page. **It is crucial that you read and attempt ALL the exercises at the end of each chapter as they form integral part of the book.**
Solve the following problems.

Problem 1. Let R be a commutative, unital ring and $a_1, \ldots, a_k$ be elements in R. Define the **the ideal** $< a_1, \ldots, a_k >$ **generated by** $a_1, \ldots, a_k$ as follows:

$$< a_1, \ldots, a_k >= \{r_1 a_1 + \ldots + r_k a_k : r_1, \ldots, r_k \in R\}$$

(so it consists of all linear combinations of $a_1, \ldots, a_k$ with coefficients in R). We say that an ideal is **finitely generated** if it is equal to $< a_1, \ldots, a_k >$ for some elements $a_1, \ldots, a_k$ in R.

a) Prove that $< a_1, \ldots, a_k >$ is indeed an ideal in R.

b) Prove that if J is an ideal in R and $a_i \in J$ for $i = 1, \ldots, k$ hen $< a_1, \ldots, a_k > \subseteq J$ (so $< a_1, \ldots, a_k >$ is the smallest ideal containing the elements $a_1, \ldots, a_k$).

c) Prove that if $I =< a_1, \ldots, a_k >$ and $J =< b_1, \ldots, b_l >$ then the ideal IJ is generated by the kl elements $a_i b_j$, $i = 1, \ldots, k$, $j = 1, \ldots, l$:

$$IJ =< a_1 b_1, a_1 b_2, \ldots, a_1 b_l, a_2 b_1, a_2 b_2, \ldots a_k b_l > .$$

d) Suppose that $I_1 \subseteq I_2 \subseteq \ldots$ is a nested sequence of ideals. Prove that the union $J = \bigcup_{i=1}^{\infty} I_i$ is an ideal. Then prove that if J is finitely generated then there is k such that $J = I_k = I_{k+1} = \ldots$.

Problem 2. Use the correspondence theorem to count the number of ideals of the ring $\mathbb{Z}_{60}$.

Problem 3. Let $f : R \longrightarrow S$ be a homomorphism of commutative unital rings.

a) Prove that if P is a prime ideal of S then $f^{-1}(P)$ is a prime ideal of R.

b) Find an example when P is a maximal ideal of S but $f^{-1}(P)$ is not maximal in R.

c) Prove that if f is onto and Q is a prime ideal of R such that $\ker f \subseteq Q$ then $f(Q)$ is a prime ideal of S.

d) Suppose that f is surjective. Prove that if P is a maximal ideal of S then $f^{-1}(P)$ is maximal in R. Prove that if Q is a maximal ideal of R then $f(Q)$ is either S or it is a maximal ideal of S.

e) Find all prime ideals of $\mathbb{Z}/36\mathbb{Z}$.

Problem 4. Let R be a commutative unital ring.

a) Prove that R is a domain iff $\{0\}$ is a prime ideal of R.

b) Prove that if P is a prime ideal and $r \in R$ is nilpotent then $r \in P$.

c) Prove that if R is finite then every prime ideal of R is maximal.

Problem 5. Let $R = \mathbb{Z}[\sqrt{n}] = \{a + b\sqrt{n} : a, b \in \mathbb{Z}\}$, where n is an integer which is not a square (so $\sqrt{n}$ is not rational).

a) Prove that R is a subring of the complex numbers $\mathbb{C}$.

b) Define a map $f : R \longrightarrow R$ by $f(a + b\sqrt{n}) = a - b\sqrt{n}$. Prove that f is an isomorphism.

c) Consider the map $N : R \longrightarrow \mathbb{Z}$ defined by $N(a + b\sqrt{n}) = a^2 - nb^2$. Prove that $N(xy) = N(x)N(y)$ for all $x, y \in R$. Prove that $x \in R$ is invertible iff $N(x) = \pm 1$. Prove that if $|N(x)|$ is a prime number then x is irreducible.

d) Prove that $\mathbb{Z}[\sqrt{2}]$ has infinitely many invertible elements. **Hint:** Consider $1 + \sqrt{2}$. Note that product of invertible elements is invertible.

e) Let p be a prime number such that $k^2 \equiv 2 \pmod{p}$ for some integer k. Let $I = p\mathbb{Z}[\sqrt{2}]$ be the princip[al ideal generated by p. Prove that neither $k + \sqrt{2}$ nor $k - \sqrt{2}$ belong to I. Use it to conclude that I is not a prime ideal.

Problem 6. Let R be an integral domain and let $a \in R$ be irrreducible but not prime. Prove that if P is a prime ideal of R and $a \in P$ then P is not principal.