The test will cover sections chapters 4, 5, 6 and 7 (thru section 7.6). There will be a review session in class on Tuesday and another review session in AB 638, 4:15-5:30, Wednesday, 29 November. Most of the following problems require carefully worded proofs. Please review past homework problems as well as the text. You will permitted one page of notes (but please do not include worked out problems).

(1) Let $f(x), g(x) \in \mathbb{Q}[x]$ be given by $f(x) = 2x^4 + x^2 - 4x + 3$ and $g(x) = x^2 + 1$. Find polynomials $q(x)$ and $r(x)$ such that $f(x) = g(x)q(x) + r(x)$, and $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

(2) Let $\varphi : R \to S$ be a homomorphism of rings and let $s \in S$ be given. Show that the map $\tilde{\varphi} : R[x] \to S$ given by

$$\tilde{\varphi}(a_0 + a_1 x + \cdots a_n x^n) = \varphi(a_0) + \varphi(a_1)s + \cdots \varphi(a_n)s^n$$

(where $a_i \in R$ for $0 \le i \le n$) is also a homomorphism. Use this fact to show that the set of all real numbers of the form $a_0 + a_1\pi + \cdots a_n\pi^n$ where $a_i \in \mathbb{Z}$ is a subring of $\mathbb{R}$.

(3) Let R be a ring with identity. Show that $R[x]$ has zero divisors if and only if R does.

(4) Use the Euclidean Algorithm to find the gcd of the given polynomials:

$$x^4 + 3x^3 + 4x + 2 \quad \text{and} \quad x^2 + 2 \quad \text{in} \quad Z_5[x].$$

(5) Show that $x^3 - 1$ and $x^2 + 1$ are relatively prime in $\mathbb{Q}[x]$.

(6) Show that $f(x) = x^3 - 2$ is irreducible in $\mathbb{Q}[x]$ but not in $\mathbb{R}[x]$. Express $f(x)$ as a product of monic irreductibles in $\mathbb{R}[x]$.

(7) Show that $x^3 + 3$ is reducible in $Z_5[x]$. Express it as a product of monic irreducibles.

(8) Find the unique factorizations into monic irreducibles of $x^4 - 1$ and $x^6 - 1$ in $\mathbb{C}[x]$ (*hint:* all factors are linear). Use these factorizations to find the gcd of $x^6 - 1$ and $x^4 - 1$ in $\mathbb{C}[x]$.

(9) Find (if possible) a quadratic polynomial in $\mathbb{Z}_6[x]$ that may be factored as a product of linear factors in two distinct ways. Is this possible in $\mathbb{Z}_7[x]$?

(10) Is $x^3 + x^2 + x + 2$ irreducible in $\mathbb{Z}_3[x]$? Is $\mathbb{Z}_3[x]/(x^3 + x^2 + x + 2)$ a field?

(11) Show that if p is a prime then $x^{p-1} - 1$ is reducible in $\mathbb{Z}_p$ and $x^{p-1} - 1 = \prod_{k=1}^{p-1} x - k$.
(*Hint:* Use the Little Fermat Theorem.)

(12) Show that, under congruence modulo $x^4 + 2x + 1$ in $\mathbb{Z}_5[x]$, there are exactly 625 distinct congruence classes.

(13) Let f be a field and let $f(x), p(x) \in F[x]$. Show that if $f(x)$ and $p(x)$ are relatively prime, then there is $g(x) \in F[x]$ such that $f(x)g(x) \equiv 1 \bmod p(x)$. Is the converse true? What does this tell you about the units in $F[x]/(p(x))$?

(14) Show that $\mathbb{Z}_5[x]/(x^3 + x + 4)$ is a field. Find, if possible, the inverse of $[x]$ in $\mathbb{Z}_5[x]/(x^3 + x + 4)$.

(15) Let $\mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$. Use the First Isomorphism Theorem to show that $\mathbb{Q}(\sqrt{3}) \simeq \mathbb{Q}[x]/(x^2 - 3)$. Is $\mathbb{Q}(\sqrt{3})$ a field?

(16) Let $a, b \in \mathbb{Z}$ be given so that a and b are not both zero and let d be the greatest common divisor of a and b in $\mathbb{Z}$. Show that $(a, b) = (d)$ (that is, the ideal generated by a and b is the same as the ideal generated by d).

(17) Let $\varphi : R \to S$ be a homomorphism of rings. Show that the kernel of φ, $K_\varphi = \{a \in R \mid \varphi(a) = 0\}$, is an ideal in R.

(18) Let I be an ideal in $\mathbb{Z}_2[x]$ such that $(x^2 + x + 1) \subseteq I \subseteq \mathbb{Z}_2[x]$. Prove that either $I = (x^2 + x + 1)$ or $I = \mathbb{Z}_2[x]$.

(19) Find all ideals in $\mathbb{Z}_{12}$. Which of these are principle?

(20) Show that every ideal in $\mathbb{Z}$ is principle.

(21) Use the First Isomorphism Theorem to show that $\mathbb{Z}_{12}/(3) \cong \mathbb{Z}_3$.

(22) Show that $x^2 + 1$ is irreducible in $\mathbb{R}$. Prove that $\mathbb{C} \cong \mathbb{R}/(x^2 + 1)$.

(23) Suppose that g is an element of a group G. Prove that $g^2 = g$ implies that $g = e$.

(24) Write down the operation table for your favorite nonabelian group.

(25) Show that every element in U_{12} other than the identity has order two. Show that $U_{12} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ by examining operation tables.

(26) Using the definition of group show that $\mathbb{T} = \{z \in \mathbb{C} \mid |z| = 1\}$ forms a group under complex multiplication. Show that for every positive integer n, $\mathbb{T}$ contains an element of order n. Show that the elements of finite order constitute a subgroup of $\mathbb{T}$. Construct a surjective homomorphism $f : \mathbb{R} \to \mathbb{T}$.

(27) For $a, b \in \mathbb{R}$ with $a \neq 0$, let $T_{a,b} : \mathbb{R} \to \mathbb{R}$ be given by $T_{a,b}(x) = ax + b$. Show that G, the collection of all such functions, forms a nonabelian group under composition (affectionately called the "$ax + b$" group). Show that the subset consisting of all such functions with $a = 1$ constitutes a normal subgroup. Show that the map $T_{a,b} \mapsto a$ defines a surjective homomorphism $G \to \mathbb{R}^*$.

(28) Let $G = \{3, 6, 9, 12\} \subseteq \mathbb{Z}_{15}$. Does G form a group under multiplication? If so, find another well-known group G is isomorphic to.

(29) Let G be a group such that $a^2 = e$ for all $a \in G$. Prove that G is abelian.

(30) Prove that $\mathbb{Z}_2 \times \mathbb{Z}_3$ is cyclic by finding a generator. Show that $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$. Is $\mathbb{Z}_2 \times \mathbb{Z}_4$ is cyclic? Show that S_3 is not cyclic.

(31) Let G be the set of all 2×2 matrices $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ such that $a, b, d \in \mathbb{R}$ and $ad \neq 0$. Prove that G is a subgroup of $GL(2, \mathbb{R})$. Is G normal? Find if possible a surjective homomorphism $f : G \to \mathbb{R}^*$. (*Hint:* There are at least two.)

(32) Show that every subgroup of a subgroup is a subgroup but not every normal subgroup of a normal subgroup is a normal subgroup. (*Hint:* Before you begin, please state the assertion to be proved a bit more precisely.)

(33) Let G be group and let $Z(G)$ denote its center. Show that every subgroup of $Z(G)$ is normal in G.

(34) Describe all cyclic subgroups of the dihedral group D_4. Show that at least one is not normal. Find a proper nontrivial subgroup which is normal.

(35) Show that the quaternion group Q is not isomorphic to the dihedral group D_4. Find if possible 5 groups of order 8 such that no two are isomorphic.

(36) Let G be a group and let $g \in G$. Show that the map $\psi : G \to G$ given by $\psi(a) = gag^{-1}$ for $a \in G$ is an automorphism. (*Hint:* You must show that it is a homomorphism and that it is bijective.) Such an automorphism is called inner.

(37) Let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ such that $a, b, c, d \in \mathbb{Z}$ and $ad - bc = 1$. Let $\varphi_A : \mathbb{Z}^2 \to \mathbb{Z}^2$ be given by

$$\varphi_A(x, y) = (ax + by, cx + dy)$$

Show that φ_A is an automorphism, but that it is not inner unless A is the identity matrix.

(38) Let $f : G \to H$ be a homomorphism of groups and let $K_f = \{a \in G \mid f(a) = e_H\}$. Prove that K_f is a normal subgroup of G (see Exercise 7.6.15). This is often a convenient way to show that a subgroup is normal.

(39) With notation as above, show that f is injective iff $K_f = \{e\}$.

(40) List the right cosets of $\langle 3 \rangle$ in $\mathbb{Z}_{15}$. Give an example of a subgroup of order 2 in D_4 and list its cosets.

(41) Find all subgroups of $G = \mathbb{Z}_{60}$. Which of these are normal? For each subgroup H, indicate its order $|H|$ and its index $[G : H]$.

(42) Show that a subgroup H of a group G is cyclic if and only if there is a homomorphism $f : \mathbb{Z} \to G$ such that $\operatorname{Im} f = H$. Show that in this case $H = \langle f(1) \rangle$.

(43) Let G be a finite group of order n. Prove that $a^n = e$ for all $a \in G$.

(44) Suppose p is prime and G is a group of order p^2. Prove that either G is cyclic or every nonidentity element has order p. Show that every proper subgroup is cyclic.

(45) Let N be a subgroup of a group G. Show that N is normal iff for every $a \in G$ and $n \in N$, there is $m \in N$ such that $ma = an$.

(46) Let H be a subgroup of a finite group G. Show that if $[G : H] = 2$, then H is normal, but that if $[G : H] = 3$, H need not be normal.