Review and Goal for Spring 2016

Definitions: Groups

1. A binary operation on G is
2. The binary operation $*$ on G is called *associative* if
3. The binary operation $*$ on G is called *commutative* if
4. The binary operation $*$ on G is said to have an *identity* if
5. Let $*$ be a binary operation G. The element $x \in G$ is said to have an *inverse* if
6. Define a group.
7. The *order* of a group is
8. Let G be a group. The order of an element of G is
9. Let G be a group. G is called an *abelian group* if
10. Define the *center* of a group. For an element in a group define the centralizer of that element. For an element in a group define the cyclic subgroup generated by that element.
11. Define a cyclic group.
12. Let H be a subset of G. Define what it means for H to be a subgroup of G: $H \leq G$.
13. Let H be a subgroup of G. What does it mean for H to be a normal subgroup of G: $H \trianglelefteq G$.
14. Let H be a subgroup of the group $(G, \dot{;} e_G)$. The relation $a \sim b$ given by $b^{-1}a \in H$ is an equivalence relation. The set of equivalence classes is called the set of left cosets and is denoted by G/H. The left coset of $a \in G$ is aH.
15. Given a group G and $g \in G$, what is the cyclic subgroup generated by g?
16. Examples of groups: S_n, A_n, D_n, Q_8, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Z}_n$, $GL(n, \mathbb{F})$, $SL(n, \mathbb{F})$, $G \times H$, G/H.
17. Define what it means for $a|b$ given $a, b \in \mathbb{Z}$.
18. Given a natural number greater than 1, say n, the definition of $\mathbb{Z}_n$ is
19. Define $U(n)$.

Definitions: Commutative Rings and Fields

A denotes a commutative ring with identity.

1. Define a ring.
2. Define a commutative ring.
3. Define a ring with identity.
4. Define a commutative ring with identity.
5. We say A is an integral domain if
6. We say A is a Principal Ideal Domain if
7. We say A is a Unique Factorization Domain if
8. We say A is a noetherian ring if
9. We say A is an artinian ring if
10. We say A is a Bézout domain if
11. We say A is a field if
12. Let $\emptyset \neq I \subseteq A$. The set I is called an (proper) ideal of A if
13. Suppose I is an ideal of A. We say I is a prime ideal if
14. Suppose I is an ideal of A. We say I is a maximal ideal if
15. Suppose $a \in A$. The principal ideal generated by a is the set
16. Suppose I is an ideal of A. We say I is a principal ideal if
17. Suppose I is an ideal of A. We say I is a finitely generated ideal if
18. Suppose $a \in A$.
    (a) We say a is a unit if
    (b) We say a is irreducible if
    (c) We say a is prime if
    (d) We say a is a zero-divisor if
    (e) We say a is a regular element if
    (f) We say a is a nilpotent element if
    (g) We say a is an idempotent if

19. Given a ring R we define $R[x]$ to be
20. Let $f(x) \in R[x]$ and suppose $f(x) = a_0 + a_1x + \cdots a_nx_n$ where $a_n \neq 0$. The constant a_n is called the (leading coefficient) and the degree of $f(x)$ is (n). We call $f(x)$ a monic polynomial if
21. Define a boolean ring.
22. Let R and S be rings and $\phi : R \to S$. We say ϕ is a ring homomorphism.
23. Given $\phi : R \to S$ a ring homomorphism the kernel of ϕ is the set $\ker\phi = \{ \qquad\qquad\qquad \}$.

Definitions: Vector Spaces

1. Suppose F is a field. An F-vector space is
2. Suppose V is an F-vector space. A subset $\mathcal{X}$ is said to be linearly independent if
3. Suppose V is an F-vector space. A subset $\mathcal{B}$ is said to be a basis if
4. Suppose V is an F-vector space. The dimension of V is
5. Let $F \leq E$ be an extension of fields. F is an E-vector space. We set $[E : F] = dim_E F$.
6. Let $F \leq E$ be an extension of fields and $\alpha \in E$. We say that α is algebraic over F if
7. Let $F \leq E$ be an extension of fields and $\alpha \in E$ be algebraic over F. What is $irr(\alpha, F)$?
8. Let $F \leq E$ be an extension of fields. We call this a finite extension if
9. Let $F \leq E$ be an extension of fields. We call this an algebraic extension if
10. An algebraically closed field is
11. Given a field F an algebraic closure of F is
12. Let $F \leq E$ be an extension of fields and $\alpha, \beta \in E$ be algebraic over F. We say α and β are conjugate if
13. Let $F \leq E$ and $\alpha \in E$. Define $F(\alpha)$.

Statements of Theorems

1. State the Division Algorithm for polynomial rings.
2. Suppose A is a commutative ring with unity. Every proper ideal of A is contained in a maximal ideal.
3. Suppose F is a field and $f(x) \in F[x]$ is a non-constant polynomial. Then $\alpha \in F$ is a root of $f(x)$ if and only if $x - \alpha$ is a factor of $f(x)$.
4. Suppose $\varphi : A \to B$ is a ring homomorphism. Then $A/\ker\varphi \cong \varphi(B)$.
5. Every PID is a UFD.
6. Suppose F is a field and $f(x) \in F[x]$ is a non-constant polynomial. There exists a field extension E of F containing a root of $f(x)$. (Note: $f(x)$ need not be irreducible.)

Proofs

1. Suppose A is a commutative ring with identity. Prove that A is an integral domain if and only if $\{0\}$ is a prime ideal.
2. Suppose A is a commutative ring with identity. Prove that A is a field if and only if A and $\{0\}$ are the only ideals of A.
3. Suppose A is a PID and let $0 \neq a \in A$ be a non-unit. Prove that a is an irreducible element if and only if aA is a prime ideal if and only if aA is a maximal ideal.
4. Suppose A is a commutative ring with unity and let I, J be ideals of A. Prove that the smallest ideal of A containing both I and J is $I + J$.
5. Prove that a finite integral domain is a field.
6. Suppose $\phi : R \to S$ is a ring homomorphism. Prove that $\ker\phi$ is an ideal of R.
7. Prove that the following are equivalent:
   - A is an integral domain.
   - $A[x]$ is an integral domain.
   - For all $0 \neq f(x), g(x) \in A[x]$, deg $[f(x)g(x)]$=deg $f(x)$ + deg $g(x)$.
8. Prove that the following are equivalent:
   - A is a field.
   - $A[x]$ is a PID.
   - Every finitely generated ideal of $A[x]$ is principally generated.
   - For every $f(x), g(x) \in A[x]$, the ideal $f(x)A[x] + g(x)A[x]$ is a principal ideal.

9. Suppose F is a field and $f(x) \in F[x]$ is of degree 2 or 3. Prove that $f(x)$ is irreducible if and only if $f(x)$ has a root in F.
10. Suppose A is a commutative ring with unity and I is a proper ideal of A. Prove that I is a prime ideal of A if and only if A/I is an integral domain.
11. Suppose A is a commutative ring with unity and I is a proper ideal of A. Prove that I is a maximal ideal of A if and only if A/I is a field.
12. Suppose $\varphi : F \to F'$ is a field homomorphism. Prove that either $\ker \varphi = \{0_F\}$ or φ is injective.
13. For a given prime p and natural number n, contruct a field of order p^n. (Explain the steps.)
14. Construct the complex numbers from the real numbers.
15. Prove that a boolean ring is commutative.
16. Suppose α is algebraic over F. prove that α^2 is algebraic over F.
17. Suppose $F \leq E$ is an extension of fields and $\alpha \in E$ algebraic over F. Prove that $[F(\alpha) : F] = \deg irr(\alpha, F)$.