*__1.__ Lemma. Suppose G be a finite abelian group such that $|G| = mn$ where m and n are relatively prime. Let $H = \{x \in G : x^n = e\}$ and $K = \{x \in G : x^m = e\}$.

Then H and K are subgroups of G and $G = H \times K \simeq H \oplus K$.

2. Lemma. Suppose G is an abelian group, p a prime, $|G| = p^n$ and $a \in G$ has maximal order. Then there exists a subgroup H of G such that $G = \langle a \rangle \times H$.

3. Theorem. If G is a finite abelian group, then G is isomorphic to the finite product of cyclic groups.

*__4.__ Theorem. If F is a finite, then F^* the nonzero elements of F are a cyclic group under multiplication.

5. Define V is a vector space over the field F, subspace, linearly dependent, linearly independent, span, basis, dimension.

6. (Exchange Lemma) Suppose for some vectors in a vector space V that $v_1, v_2, \ldots, v_{k+1}$ are linearly independent, and span$(\{v_1, \ldots, v_k, w_1, \ldots, w_m\}) = V$. Then for some i span$(\{v_1, \ldots, v_{k+1}, w_1, \ldots, w_{i-1}, w_{i+1}, \ldots w_m\}) = V$.

*__7.__ Theorem. If a vector space V can be spanned by n vectors, then any set of $n+1$ vectors in V is linearly dependent.

8. Theorem. Any two bases of a vector space V have the same size.

*__9.__ Theorem. If F is a field and $f(x) \in F[x]$ is a polynomial, then there exists a field $E \supseteq F$ and $\alpha \in E$ such that $f(\alpha) = 0$.

10. Theorem. If F is a field and $f(x) \in F[x]$ is a polynomial of degree n, then there exists a field $E \supseteq F$ and $\alpha_i \in E$ such that $f(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$.

11. For a field F and α in an extension field of F define $F(\alpha)$.

*__12.__ Theorem. If $p(x)$ is an irreducible polynomial of degree n in $F[x]$ and α a root of p in some extension field, then

$$F(\alpha) = \{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} : a_0, \ldots, a_{n-1} \in F\}$$

13. Theorem. If $p(x) \in F[x]$ is an irreducible polynomial and α a root of p in some extension field, then there is an isomorphism $\sigma : F[x]/\langle p(x) \rangle \to F(\alpha)$ such that $\sigma(a + \langle p(x) \rangle) = a$ for each $a \in F$ and $\sigma(x + \langle p(x) \rangle) = \alpha$.

14. Theorem. If $p(x) \in F[x]$ is an irreducible polynomial and α and β are two roots of p, then $F(\alpha) \simeq F(\beta)$ with an isomorphism which fixes F and takes α to β.

*$\mathbf{15.}$ Theorem. Minimal polynomials are irreducible: If α is in some extension field of F and define:

$$I = \{f(x) \in F[x] : f(\alpha) = 0\}$$

Then:
(a) I is an ideal in $F[x]$
(b) (assuming I is nontrivial) $I = \langle p(x) \rangle$ where $p(x)$ is any polynomial of minimal positive degree in I and
(c) $p(x)$ is irreducible and so I is a maximal ideal.

16. For fields $F \subseteq E$ define $[E : F]$.

*$\mathbf{17.}$ Theorem. If $p(x)$ is an irreducible polynomial of degree n in $F[x]$ and α a root of p in some extension field, then $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ is a basis for $F(\alpha)$ as a vector space over F and hence $[F(\alpha) : F] = n$.

*$\mathbf{18.}$ Theorem. If $F_1 \subseteq F_2 \subseteq F_3$ are fields then $[F_3 : F_1] = [F_3 : F_2][F_2 : F_1]$ and furthermore the left side is infinite iff at least one of the two on the right is infinite.

19. Define $\alpha \in \mathbb{R}$ is constructible using straight edge and compass.

20. Theorem. The set of constructible numbers is a field F_c such that for any $\alpha \in F_c$ with $\alpha > 0$ we have $\sqrt{\alpha} \in F_c$.

*$\mathbf{21.}$ Theorem. α is constructible iff there exists an n and fields F_i

$$\mathbb{Q} = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n \subseteq \mathbb{R}$$

such that $\alpha \in F_n$ and for each $k = 0, \ldots, n-1$ there exists α_k such that $\alpha_k^2 \in F_k$ and $F_{k+1} = F_k(\alpha_k)$.

*$\mathbf{22.}$ Theorem. If α is constructible, then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^n$ for some integer n.

*$\mathbf{23.}$ Theorem. $^3\sqrt{2}$ is not constructible.

24. Theorem. The angle of 20 degrees is not constructible.

25. Theorem. π is not constructible.

26. Define α is algebraic over F.

*$\mathbf{27.}$ Theorem. If $[E : F] < \infty$, then every $\alpha \in E$ is algebraic over F.

*$\mathbf{28.}$ Theorem. If $F \subseteq E$ are fields and $K = \{\alpha \in E : \alpha \text{ is algebraic over } F\}$ then K is a subfield of E.

29. Define α is a multiple root of $f(x)$, define $f'(x)$.

*__30.__ Theorem. Suppose $f(x) \in F[x]$ and α is root of $f(x)$ in some extension of F. Then α is a multiple root of f iff α is a root of f'.

*__31.__ Theorem. Suppose char(F)=0 and $p(x) \in F[x]$ is irreducible, then p does not have any multiple roots.

32. Lemma. Suppose char(F)=0 and $[F(\alpha, \beta) : F] < \infty$. Then there exist γ such that $F(\alpha, \beta) = F(\gamma)$.

*__33.__ Theorem. Suppose char(F)=0 and $[E : F] < \infty$, then there exists $\alpha \in E$ such that $E = F(\alpha)$.

34. Theorem. Suppose $F \supseteq \mathbb{Z}_p$ is a finite field and $[F : \mathbb{Z}_p] = n$, then
$(F, +) \simeq \mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p = \mathbb{Z}_p^n$ and so $|F| = p^n$.

*__35.__ Theorem. Given p a prime and n a positive integer, there exists a field F with $|F| = p^n$.

36. Define E is a splitting field of the polynomial $f(x)$ over F.

*__37.__ Theorem. If $|F| = p^n$ is a field with $F \supseteq \mathbb{Z}_p$, then F is a splitting field of the polynomial $f(x) = x^{p^n} - x$ over $\mathbb{Z}_p$.

38. Lemma. If $\sigma : F \to F'$ is an isomorphism, $p(x) \in F[x]$ irreducible, $p(\alpha) = 0$, and $\sigma(p)(\beta) = 0$ in some extension fields, then there exists an isomorphism $\rho \supseteq \sigma$ such that $\rho : F(\alpha) \to F'(\beta)$ and $\rho(\alpha) = \beta$.

39. Lemma. If $\sigma : F \to F'$ is an isomorphism, $f \in F[x]$ any polynomial, $E \supseteq F$ a splitting field of f over F, and $E' \supseteq F'$ a splitting field of $\sigma(f)$ over F', then there exists an isomorphism $\rho \supseteq \sigma$ such that $\rho : E \to E'$.

40. Theorem. Splitting fields are unique up to isomorphism, i.e., if E_1 and E_2 are splitting fields of $f(x) \in F[x]$, then there exists an isomorphism $\phi : E_1 \to E_2$ which is the identity on F.

*__41.__ Theorem. Any two finite fields of the same size are isomorphic.