Algebra Qualifying Exam Notes

Proposition 1: *Let H be a subgroup of G of index p, where p is the smallest prime dividing the order of G. Then H is a normal subgroup of G*

Proposition 2: *G/N is abelian $\Leftrightarrow [G,G] \leq N$*

Proof: ($\Rightarrow$) Let $a, b \in G$. Then $[a,b]N = [aN, bN] = N$. So $[a,b] \in N$. Thus N contains all commutators. So N contains $[G,G]$, the subgroup generated by all commutators. Then, of course, $[G,G] \leq N$.

($\Leftarrow$) Let $a, b \in G$. Then $[aN, bN] = [a,b]N = N$, since $[a,b] \in [G,G] \subseteq N$. Therefore, G/N is abelian.QED

Proposition 3: *If H, K are subgroups of G and $H \leq N_G(K)$, then HK is a subgroup of G*

Corollary 4: *If H, K are subgroups of G and one of them is normal in G, then HK is a subgroup of G.*

Second isomorphim theorem: If $H \leq G, N \trianglelefteq G$, then $HN/N \cong H/(H \cap N)$

Proposition 5: *If G is a simple group and H is a proper subgroup of G of index n, then there is an injective homomorphisms $\phi : G \to S_n$.*

Proof: Let G act on the cosets of H by left multiplication. This action permutes the cosets of H. So it induces a homomorphism $\phi : G \to S_{[G:H]} \cong S_n$. Note that ϕ is not the trivial homomorphism. Otherwise, $gH = H$ for all $g \in G$ meaning that $H = G$. Therefore, $\ker \phi \neq G$. But $\ker \phi$ is a normal subgroup of G. Since G is simple, the only other option is for $\ker \phi$ to be trivial. Therefore, ϕ is injective. QED

Definition: The orbit of x is $G \cdot x = Orb_G(x) := \{g \cdot x | g \in G\}$

Definition: The stabilizer of x is $G_x = Stab_G(x) := \{g \in G : g \cdot x = x\}$

Orbit stabilizer theorem: $|Orb_G(x)| = [G : Stab_G(x)] = |G|/|Stab_G(x)|$

Proof: Let $\phi : G/Stab_G(x) \to Orb_G(x)$ be defined by $\phi(gStab_G(x)) = g \cdot x$. First let's check that this is well-defined. If $gStab_G(x) = g'Stab_G(x)$, then $g = g'h$ for some $h \in Stab_G(x)$. So $\phi(gStab_G(x)) = g \cdot x = g'h \cdot x = g' \cdot x = \phi(g'Stab_G(x))$. Thus the map is well-defined. ϕ is clearly surjective, since any element of $Orb_G(x)$ can be written in the form $g \cdot x = \phi(gStab_G(x))$. Also if $\phi(gStab_G(x)) = \phi(g'Stab_G(x))$, then $g \cdot x = g' \cdot x$. So $g^{-1}g' \cdot x = x$. Thus, $g^{-1}g' \in Stab_G(x)$. So $gStab_G(x) = gg^{-1}g'Stab_G(x) = g'Stab_G(x)$. Therefore, ϕ is also injective. So ϕ is a bijcetion. Thus, $|Orb_G(x)| = |G/Stab_G(x)|$. QED

Definition: The centralizer of a nonempty subset A of a group G is $C_G(A) = \{g \in G | gag^{-1} = a, \forall a \in A\}$. It is a subgroup of G.

Definition: The normalizer of a nonempty set A of a group G is $N_G(A) = \{g \in G | gAg^{-1} = A\}$. It is a subgroup of G.

Proposition 6: $C_G(A) \leq N_G(A)$

Proposition 7: *The number of conjugates of an element $g \in G$ is $[G : C_G(g)]$*

Proof: This follows from the orbit-stabilizer theorem. QED

Sylow's theorems

1. All Sylow p-subgroups are conjugate.
2. $n_p(G)||G|$ and $n_p(G) \equiv 1 \mod p$. In particular, $n_p(G) = [G : N_G(P)]$ where P is a Sylow p-subgroup

Semidirect Products: Let G be a group. If N is a normal subgroup of G, H is a subgroup of G, $NH = G$, and $N \cap H = \{e\}$, then $G \cong N \rtimes H$.

Fratini's Argument: Let G be a finite group. Let H be a normal subgroup of G, and let P be a Sylow p-subgroup of H. Then $G = HN_G(P)$ and $|G : H|$ divides $|N_G(P)|$.

Proof: Since H is normal in G, $HN_G(P)$ is a subgroup of G. For any $g \in G$, $gPg^{-1} \leq gHg^{-1} = H$. Thus, gPg^{-1} is a Sylow p-subgroup of H. All Sylow p-subgroups of H are conjugate in H, so there exists an $h \in H$ such that $hPh^{-1} = gPg^{-1}$. Thus $h^{-1}gP(h^{-1}g)^{-1} = P$. So $h^{-1}g \in N_G(P)$. Therefore, $g \in hN_G(P)$. So $G \leq HN_G(P)$. Therefore, $G = HN_G(P)$.

By the second isomorphism theorem, $[G : H] = |G/H| = |HN_G(P)/H| = |N_G(P)/(N_G(P) \cap H| = |N_G(P)|/|N_G(P) \cap H|$. So $[G : H]$ divides $|N_G(P)|$. QED

Definition: The upper central series of a group G is the chain of subgroups $1 = Z_0(G) \leq Z_1(G) \leq Z_2(G) \leq \cdots$ such that $Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$.

Definition: The lower central series of a group G is the chaing of subgroups $G^0 \geq G^1 \geq G^2 \geq \cdots$, where $G^0 = G, G^1 = [G, G]$, and $G^{i+1} = [G, G^i]$.

Definition: A group G is nilpotent if $Z_c(G) = G$. (Equivalently, A group G is nilpotent if $G^c = 1$) The smallest such c is the nilpotence class of G

Theorem 8: *Let G be a finite group. The following are equivalent:*

1. *G is nilpotent*
2. *Every proper subgroup of G is a proper subgroup of its normalizer*

3. *Every Sylow Subgroup is normal in G*

4. *G is a direct product of its Sylow subgroups*

5. *Every maximal subgroup of G is normal.*

Definition: The derived or commutator subgroup of a group G is $[G, G]$

Definition: The derived or commutator series of a group is the sequence
$G^{(0)} = G,\ G^{(1)} = [G, G],\ G^{(i+1)} = [G^{(i)}, G^{(i)}]$. The notation $G' = G^{(1)}$ and $G'' = G^{(2)}$ is also used.

Definition: A group G is solvable if there is a chain of subgroups $1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_s = G$ Such that G_{i+1}/G_i is abelian for all i

Proposition 9: *G is solvable $\Leftrightarrow$ $G^{(n)} = 1$ for some $n \geq 0$.*

Proposition 10: *If $N \trianglelefteq G$ is solvable and G/N is solvable, then G is solvable.*

Proposition 11: *$G^{(i)} \leq G^i$ for all i*

Proposition 12: *If G is nilpotent, then G is solvable.*

Properties of S_n:

Proposition 13:

1. *The transitive subgroups of S_4 are S_4, A_4, D_4, V_4, C_4.*
2. *The transitive subgroups of S_3 are S_3 and A_3.*

Proposition 14: *For all $n \geq 3, n \neq 4$, A_n is the only nontrivial proper normal subgroup of S_n. For $n = 4$, S_n also has the normal subgroup $\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ isomorphic to V_4.*

Proof: (For $n \geq 5$ only) Let H be a nontrivial proper normal subgroup of S_n. Then $H \cap A_n \trianglelefteq A_n$. A_n is simple for $n \geq 5$, so $H \cap A_n = A_n$ or 1. Suppose $H \cap A_n = 1$. Since H, A_n are both normal in S_n, we have that HA_n is a supgroup of S_n and $HA_n/A_n = H/(H \cap A_n) \cong H$. So $2 = |S_n/A_n| \geq |HA_n/A_n| = |H| > 1$. Therefore, $|H| = 2$. So $H = \langle \sigma \rangle$ for some nontrivial σ of order 2. Since H is also normal in S_n, conjugating σ by any element of S_n must be σ. Thus, $\sigma \in Z(S_n)$. But $Z(S_n) = \{e\}$ for $n \geq 3$. So we have a contradiction. Therefore, $H \cap A_n = A_n$. So $A_n \leq H$. In fact, $A_n \trianglelefteq H$, since A_n is normal in S_n. Thus, $H/A_n \leq S_n/A_n$. So $|H/A_n| \leq |S_n/A_n| = 2$. Therefore, $|H| = |A_n|$ or $|H| = 2|A_n| = |S_n|$. Thus, $H = A_n$ or S_n. Since H is a proper subgroup of S_n. $H = A_n$. QED

Proposition 15: $Z(S_n) = \{e\}$ *for* $n \geq 3$

Proof: Let $\sigma \in S_n \setminus \{e\}$. Then there exists an i, j with $i \neq j$ such that $\sigma(i) = j$. Let $k \in \{1, 2, ..., n\}$ with $i \neq k \neq j$. Then $(i\ k)\sigma(i) = j \neq \sigma(k) = \sigma(i\ k)(i)$. Therefore, σ does not commute with $(i\ k)$. So $\sigma \notin Z(S_n)$. Therefore, $Z(S_n)$ can at most contain the identity element, which it of course does. Thus, $Z(S_n) = \{e\}$. QED

Proposition 16: $[S_n, S_n] = A_n$

Proof: This is trivial for $n = 1, 2$. For $n \geq 3, \neq 4$, A_n is the only nontrivial proper normal subgroups of S_n. $[S_n, S_n]$ is the smallest normal subgroup of S_n such that $S_n/[S_n, S_n]$ is abelian. $S_n/A_n \cong C_2$ is abelian. The only smaller subgroup of S_n is $\{e\}$, and $S_n/\{e\} \cong S_n$ is not abelian. Therefore, $[S_n, S_n] = A_n$. Similarly, for $n = 4$, $[S_n, S_n]$ is either A_n or the normal subgroup $\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \cong V_4$. $[(1\ 2\ 3), (1\ 4)] = (1\ 2\ 3)(1\ 4)(1\ 3\ 2)(1\ 4) = (1\ 2\ 4)$. Therefore, $(1\ 2\ 4) \in [S_n, S_n]$. As $(1\ 2\ 4)$ is not in the subgroup isomorphic to V_4, $[S_n, S_n] = A_n$. QED

Properties of A_n:

Proposition 17: A_n *is a non-abelian simple group for all* $n \geq 5$

Proposition 18: $A_4 \cong V_4 \rtimes C_3$

Proposition 19: *For all* $n \geq 3, n \neq 4$, A_n *is a simple group. For* $n = 4$, $\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ *isomorphic to* V_4 *is the only nontirivial proper normal subgroup of* A_n.

Proof: (For $n = 4$ only) I will show that the only nontrivial proper normal subgroup of $V_4 \rtimes C_3$ is V_4. Let $N \neq V_4$ be a nontrivial normal subgroup of $V_4 \rtimes C_3$. N is not a subgroup of V_4 (Simple multiplications that $N = V_4$ if that is the case). Therefore, N contains an element of the form vn where $v \in V_4, n \in C_3 \setminus \{0\}$. Such an element has order 3. The Sylow 3-subgroups of $V_4 \rtimes C_3$ have order 3. Thus, N contains a Sylow 3-subgroup of $V_4 \rtimes C_3$. Since Sylow 3-subgroups are conjugate and N is normal, N conatins all Sylow 3-subgroups.$n_3(V_4 \rtimes C_3) = 1$ or 4. If $n_3(V_4 \rtimes C_3) = 1$, then the semi-direct product would just be a direct product. Thus, $n_3(V_4 \rtimes C_3) = 4$. The intersection of distinct Sylow 3-subgroups is trivial. Otherwise, they would be the same, since every nontrivial element of a group of order 3 generates the group. Thus, there are $9 = 3 \cdot 4 - 3$ elements in total in the Sylow 3-subgroups. So $|N| \geq 9$ and $|N|$ divides 12. Therefore, $|N| = 12$. So $N = V_4 \rtimes C_3$. Therefore, the only nontrivial subgroup of $V_4 \rtimes C_3$ not equal to V_4 is the improper one. QED

Proposition 20: *For* $n \geq 4$, $Z(A_n) = \{e\}$

Proof: $Z(A_n)$ is a normal subgroup of A_n. For $n \geq 5$, A_n is simple, so $Z(A_n) = A_n$ or $\{e\}$. But A_n is not abelian for $n \geq 5$, so $Z(A_n) = \{e\}$. For $n = 4$, $Z(A_n) = \{e\}$ or $\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$, since A_4 is not abelian. $(1\ 2)(3\ 4)$ and $(1\ 2\ 3)$ don't commute. Thus, $Z(A_n) = \{e\}$. QED

Proposition 21: $[A_n, A_n] = A_n$ *for* $n \geq 5$. $[A_4, A_4] = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \cong V_4$.

Proof: $[A_n, A_n]$ is a normal subgroup of A_n. For $n \geq 5$, A_n is simple, so $[A_n, A_n] = A_n$ of $\{e\}$. But An is not abelian for $n \geq 5$, so $[A_n, A_n] = A_n$. For $n = 4$, $[A_n, A_n] = A_n, \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$, or $\{e\}$. $[A_n, A_n] \neq \{e\}$ because A_n is not abelian. $A_n/\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \cong C_3$, which is abelian. Since A_n is the only other normal subgroup of A_n, $\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ is the smallest normal subgroup such that $A/\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ is abelian. Therefore, $[A_4, A_4] = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \cong V_4$. QED

Definition: $\mathrm{Aut}(G)$ is the set of all automorphisms of a group G

Definition: $\mathrm{Inn}(G)$ is the set of all inner automorphisms. Those that arise as conjugation by an element in G.

Definition: $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$

Proposition 22: $Inn(G) \cong G/Z(G)$

Definition: The characteristic polynomial of a matrix A is $C_A(x) = \det(xI - A)$

Definition: The minimal polynomial of a matrix A is the unique monic polynomial of smallest degree which when evaluated at A is zero. It is denoted $m_A(x)$.

Proposition 23:

1. *The characteristic polynomial of A is the product of the invariant factors of A*
2. *The minimal polynomial divides the characteristic polynomial of A*
3. *The minimal polynomial contains all the roots*
4. *The degree of the minimal polynomial of an $n \times n$ matrix A is at most n.*
5. *The degree of the characteristic polynomial of an $n \times n$ matrix A is n.*

Definition: The invariant factors are the diagonal elements in the Smith Normal form with degree at least one. The invariant factors $a_1(x), ..., a_m(x)$ satisfy $a_i(x)|a_{i+1}(x)$. $a_m(x)$ is the minimal polynomial.

Definition: The companion matrix of an invariant factor $a(x) = \sum_{i=1}^{n} a_i x^i$ is $\begin{pmatrix} 0 & \cdots & \cdots & 0 & -a_0 \\ 1 & \ddots & & \vdots & -a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{n-2} \\ 0 & \cdots & 0 & 1 & -a_{n-1} \end{pmatrix}$

The rational canonical form of a matrix is the block diagonal matrix whose blocks are the companion matrices of the invariant factors. If a matrix is in such a form, then the campanion matrices are automomatically the companion matrices of the invariant factors.

Definition: The elementary divisors are obtained from the invariant factors by writing each invaraint factors as the product of distinct linear factors to powers; these linear factors to their respective powers are the elementary divisors. For example, if $(x-1)(x-3)^3, (x-1)(x-2)(x-3)^3, (x-1)(x-2)^2(x-3)^3$ are the invariant factors, then the elementary divisors are $(x-1), (x-3)^3, (x-1), (x-2), (x-3)^3, (x-1), (x-2)^2, (x-3)^3$

Definition: The Jordan block of $(x-\lambda)^k$ is the $k \times k$ matrix $\begin{pmatrix} \lambda & 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \ddots & 1 \\ 0 & \cdots & \cdots & 0 & \lambda \end{pmatrix}$

The Jordan canonical form of a matrix is the block diagonal matrix whose blocks are the Jordan blocks of the elementary divisors.

Proposition 24: *Similar matrices have the same RCF and JCF*

Proposition 25: *A matrix is diagonalizable iff its minimal polynomial factors into linear factors over the field.*

Proof: If its minimal polynomial factors into linear factors over the field, then so do all of the invariant factors. Thus all the elementary divisors are linear. Therefore, the Jordan canonical form of the matrix is diagonal. So the matrix is diagonalizable. For the converse, if a matrix is diagonalizable, its elementary divisors are all linear. So the invariant factors, in particular the minimal polynomial, factor into linear factors over the field. QED

$\phi(n) = \deg(\Phi_n(x))$ and cyclotomic polynomials
$\phi(p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}) = (p_1)^{n_1-1}(p_1-1)(p_2)^{n_2-1}(p_2-1)\cdots(p_k)^{n_k-1}(p_k-1)$, where the p_i are distinct primes.

Lemma 26: *Over an algebraically closed field if $W \neq 0$ is an invariant subspace of V under B, then W has an eigenvector in B.*

Proof: There is a linear transormation $T : W \to W$ that corrsponds to left multiplication by B. Choose a basis for W and extend it to a basis for V. Let B' be B with respect to this basis. The matrix B'' corresponding to T will be of smaller order than B', because B' acts on a larger space. In fact, B'' is a submatrix of B'. The characteristic polynomial of B'' has a root in the algebraically closed field. Thus B'' has an eigenvalue λ, and hence and eigenvector $v \in W$. Thus, $T(v) = \lambda v$. So $Bv = T(v) = \lambda v$. Thus, B has an eigenvector in W.QED

Spectral Theorem:

1. Hermitian matrices (ones that equal their conjugate transpose) are diagonalizable over $\mathbb{C}$
2. Symmetric matrices are diagonalizable over $\mathbb{R}$

Proof: Let A be a hermitian matrix. Then A has an eigenvector v_1 with eigenvalue λ. Let W_1 be the subspace of all vectors orthogonal to v_1. For any $w \in V_1$, $\langle v_1, Aw\rangle = \langle Av_1, w\rangle = \lambda\langle v_1, w\rangle = 0$. Thus, $Aw \in W_1$. Therefore, W_1 is an invariant subspace of A. So A has an eigenvector $v_2 \in W_1$. Let W_2 be the subspace of W_1 consisting of all vectors orthogonal to v_2. Repreat this process, to get a set of orthongal vectors. These are necessarily linearly independent, so they form a basis for V. (If $\sum_{i=1}^n a_i v_i = 0$, then $a_j = \langle v_j, \sum_{i=1}^n a_i v_i\rangle = \langle v_j, 0\rangle = 0$.) With respect to this basis, A is diagonal. The same holds for symmetric matrices. That is, they are diagonalizable over $\mathbb{C}$. To show they are diagonalizable over R, it is sufficient to show that the eigenvalues must all be real. Note that the real component of any eigenvector is an eigenvector if this is the case. Let v be an eigenvector of A with norm 1 and eigenvalue λ. Then $\lambda = \lambda\langle v, v\rangle = \langle Av, v\rangle = \langle v, Av\rangle = \langle v, \lambda v\rangle = \bar{\lambda}\langle v, v\rangle = \bar{\lambda}$. So λ is real. QED

Definition: M is a Noetherian R-module if any increasing chain of submmodules stabilizes.

Proposition 27: *M is a Noetherian R-module iff every submodule of M is finitely generated.*

Example of a finitely generated module that is not Noetherian: $\mathbb{Q}[x_0, x_1, ...]$ has submodule $\langle x_0, x_1, ...\rangle$, which is not finitely generated.

The dimension of a free module over a commutative ring with unity is invariant.
Distribution with tensor products: $(\sum_{i=1}^m M_i) \otimes (\sum_{j=1}^n N_j) = \sum_{i,j} M_i \otimes N_j$

Definition: $\phi : M \times N \to L$ is R-balanced if it is bilinear and $\phi(mr, n) = \phi(m, rn)$

The universal property of tensor products: Let $\phi : M \times N \to L$ be an R-balanced map, where R is a ring with unity, M is a right R-module, N is a left R-module, L is an R-moduule. Then there is a unique R-module homomorphism $\Phi : M \otimes_R N \to L$ such that $\Phi(m \otimes n) = \phi(m, n)$.

$C_m \otimes_{\mathbb{Z}} C_n \cong C_{gcd(m,n)}$. Prove this using the map $\phi : C_m \times C_n \to C_{gcd(m,n)}$ defined by $\phi(a, b) = ab$ mod $gcd(m, n)$.

Chinese remainder theorem

1. Let n be a positive integer and let $p_1^{n_1} \cdots p_k^{n_k}$ be its factorization into powers of distinct primes. Then $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{n_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{n_k}\mathbb{Z}$.
2. Let $g(x)$ be a nonconstant monic polynomial in $F[x]$, where F is a field, and let $f_1(x)^{n_1} \cdots f_k(x)^{n_k}$ be its factorization into powers of distinct irrducible polynomials. Then $F[x]/(g(x)) \cong F[x]/(f_1(x)^{n_1}) \times \cdots \times F[x]/(f_k(x)^{n_k})$.

Definition: A module is simple if it has no nontrivial proper submodules.

Definition: A nonzero ring R with unity is semisimple if it is isomorphic to a finite direct sum of simple modules.

Definition: Division rings are essentially fields with multiplication that is not commutative

Proposition 28: *Finite division rings are fields*

Artin-Wedderburn Theorem: Let R be a semisimple nonzero ring with unity (not necessarily commutative). Then $R \cong \Pi_{i=1}^{k} M_{n_i}(D_i)$ where the D_i are division rings.

Proposition 29: *PID $\Rightarrow$ UFD. It follows that PID $\Rightarrow$ Noetherian*

Proposition 30:
1. *R is an integral domain $\Rightarrow$ $R[x]$ is an integral domain*
2. *R is a UFD $\Leftrightarrow$ $R[x]$ is a UFD*
3. *R is a PID $\Rightarrow$ $R[x]$ is a UFD*
4. *F is a field $\Rightarrow$ $F[x]$ is a PID*

Counterexample: $\mathbb{Z}$ is a PID, but $\mathbb{Z}[x]$ is not. Consider $(2, x)$.

Definition: For any submodule N of M.
The annihilator of N is $\text{Ann}(N) = \{r \in R : rn = 0, \forall n \in N\}$. It is an ideal of R.

Eisenstein Criterion: Let $p \in \mathbb{Z}$ be prime. $f = \sum_{i=1}^{n} a_i x^i \in \mathbb{Z}[x]$ is Eisenstein if $a_n \notin p\mathbb{Z}$, all other $a_i \in p\mathbb{Z}$ and $a_0 \notin p^2\mathbb{Z}$. If f is Eisenstein, it is irreducible in $\mathbb{Q}[x]$. If f is also primitive (i.e. the gcd of its coefficients is 1), then it is irreducible in $\mathbb{Z}[x]$.

Proposition 31: *$F(\alpha)/F$ is algebraic iff α is algebraic over F.*

Definition:
1. A polynomial is separable if all of its roots are have multiplicity 1.
2. $\alpha \in E$ is separable over F if its minimal polynomial is separable.
3. E/F is separable if every $\alpha \in E$ is separable over F.

Proposition 32: *Let K/F be algebraic. Then K/F is separable iff K/E and E/F are separable.*

Primitive Element Theorem: EVery finite separable field extension E/F is simple. That is, $E = F(\alpha)$.

Definition: E/F is normal if it is the splitting field of some set of polynomials.

Proposition 33: *Let $K/E/F$. Then K/F normal implies that K/E is normal*

Proposition 34: *E/F and K/F normal implies EK/F normal*

Definition: A field extension K/F is Galois if it is both normal and separable

Proposition 35: *K/F is Galois iff K is the splitting field of some separable polynomial over F.*

Proposition 36: *If $f(x) \in \mathbb{Q}[x]$ has degree n and K is the splitting field of f over $\mathbb{Q}$, then $Gal(K/\mathbb{Q})$ is isomorphic to a transitive subrgroup of S_n.*

Proposition 37: $|Gal(E/F)| = [E : F]$

Definition: For $G \leq \mathrm{Gal}(E/F)$, E^G is the largest subfield of E fixed by G.

Proposition 38: $Gal(K/K^H) = H$

Fundamental Theorem of Galois Theory: There is a one to one correspondence of intermediate fields of K/F and subgroups of $\mathrm{Gal}(K/F)$ with normal extensions E/F corresponding to normal subgroups. $H \leq \mathrm{Gal}(K/F)$ corresponds to K^H.

Proposition 39: *$Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, where ζ_n is a primitive nth root of unity.*

Proposition 40:

1. *If p is an odd prime, then $(\mathbb{Z}/p^n\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{n-1}\mathbb{Z}$.*
2. *If p is an even prime, then $(\mathbb{Z}/p^n\mathbb{Z})^\times \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^{n-2}\mathbb{Z}$*

Proposition 41:

1. *$\mathbb{F}_{p^n}$ is a field of roots of $x^{p^n} - x$.*
2. *All finite fields are of the form $\mathbb{F}_{p^n}$.*

3. *The Galois group of $\mathbb{F}_{p^n}/\mathbb{F}_p$ is cyclic of order n and is generated by the Frobenius map: $x \mapsto x^p$.*

4. $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m} \Leftrightarrow n|m$

Proposition 42: *The squareroots of distinct primes are linearly independent.*

Descartes rule of signs: Roots with multiplicity great than 1, are counted multiple times.

1. Positive roots = # of sign changes of coefficients or some multiple of 2 less
2. Negative roots = # of sign changes of coefficients or some multiple of 2 less after multiplying odd terms by -1

Cramer's rule: If $Av = B$ where A is an $n \times n$ matrix and v, B are vectors, then $v_i \det A = \det A'$ where A' is the matrix A with the ith column replaced by B.

Vandermonde determinant formula: $\begin{vmatrix} 1 & 1 & \cdots & 1 & 1 \\ x_1 & x_2 & \cdots & x_{n-1} & x_n \\ x_1^2 & x_2^2 & \cdots & x_{n-1}^2 & x_n^2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ x_1^{n-1} & x_2^{n-1} & \cdots & x_{n-1}^{n-1} & x_n^{n-1} \end{vmatrix} = \Pi_{1 \le i < j \le n}(x_j - x_i)$

Proof: Subtract the nth column from all the other columns. To get

$$\begin{vmatrix} 1 & 1 & \cdots & 1 & 1 \\ x_1 & x_2 & \cdots & x_{n-1} & x_n \\ x_1^2 & x_2^2 & \cdots & x_{n-1}^2 & x_n^2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ x_1^{n-1} & x_2^{n-1} & \cdots & x_{n-1}^{n-1} & x_n^{n-1} \end{vmatrix} = \begin{vmatrix} 0 & 0 & \cdots & 0 & 1 \\ x_1 - x_n & x_2 - x_n & \cdots & x_{n-1} - x_n & x_n \\ x_1^2 - x_n^2 & x_2^2 - x_n^2 & \cdots & x_{n-1}^2 - x_n^2 & x_n^2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ x_1^{n-1} - x_n^{n-1} & x_2^{n-1} - x_n^{n-1} & \cdots & x_{n-1}^{n-1} - x_n^{n-1} & x_n^{n-1} \end{vmatrix}$$

Multiplty the $(n-1)$th row by $-x_n$ and add it to the n row. Repeat this by multipltying the $(i-1)$th row by $-x_n$ and add it to the i row. This gets us

$$= \begin{vmatrix} 0 & 0 & \cdots & 0 & 1 \\ x_1 - x_n & x_2 - x_n & \cdots & x_{n-1} - x_n & 0 \\ (x_1 - x_n)x_1 & (x_2 - x_n)x_2 & \cdots & (x_{n-1} - x_n)x_{n-1} & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ (x_1 - x_n)x_1^{n-2} & (x_2 - x_n)x_2^{n-2} & \cdots & (x_{n-1} - x_n)x_{n-1}^{n-1} & 0 \end{vmatrix}$$

Pulling out the factors of $x_i - x_n$ we get

$$= \Pi_{1 \le i < n}(x_n - x_i) \times (-1)^{n-1} \begin{vmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 1 & \cdots & 1 & 0 \\ x_1 & x_2 & \cdots & x_{n-1} & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ x_1^{n-2} & x_2^{n-2} & \cdots & x_{n-1}^{n-1} & 0 \end{vmatrix} = \Pi_{1 \le i < n}(x_n - x_i) \times \begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_{n-1} \\ \vdots & \vdots & \vdots & \vdots \\ x_1^{n-2} & x_2^{n-2} & \cdots & x_{n-1}^{n-1} \end{vmatrix}$$

So the Vandermonde determinanat formula is true for an $n \times n$ matrix if it is true for an $(n-1) \times (n-1)$ matrix. It is also true for $n = 2$. So by induction it is true for all $n \ge 2$. QED

Definition: An R-algebra A is a ring with unity along with multiplication by elements in R and this multiplication is commutative: $r \cdot a = a \cdot r$.