Math 553 Qualifying Exam

August, 2018 Ron Ji

In this test, $e$ denotes the identity element of a group; $|g|$ denotes the order of the group element $g$ and $K/F$ denotes the field extension $K$ of $F$.

Even if you may not be able to prove certain parts, you may still use them to prove other statements following them.

1. Let $G$ be an abelian group and let $a_1, a_2, ..., a_n$ be elements of finite order. Show that there is an element $a$ in $G$ such that $|a| = \text{lcm}(|a_1|, |a_2|, ..., |a_n|)$.

2. Let $G$ be a finite group of order $n$. Define $S_m = \{g \in G | g^m = e\}$ for an integer $m > 1$. Suppose $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, where $p_i$’s are distinct prime numbers and $a_i$’s are natural numbers. Assume $|S_m| \leq m$ for $m = p_i^{t_i}$, where $i = 1, 2, ..., k$ and $t_i \leq a_i$. Prove the following.
   (a) Each Sylow $p_i$-subgroup $P_i$ of $G$ is normal.
   (b) $G$ is isomorphic to the direct product of the Sylow $p_i$-subgroups of $G$, for $i = 1, 2, ..., k$.
   (c) Each Sylow $p_i$-subgroup of $G$ is cyclic.
   (d) $G$ is cyclic.

3. Let $R$ be a domain with identity satisfying the following three conditions.
   (a) For each pair of nonzero elements $x$ and $y$ in $R$, $\gcd(x, y)$ exists.
   (b) For every pair of elements $x$ and $y$ in $R$, there are $s$ and $t$ in $R$ such that $sx + ty = \gcd(x, y)$.
   (c) For a chain of principal ideals $(x_1) \subset (x_2) \subset (x_3) \subset \cdots$ in $R$, $\bigcup_{n=1}^\infty (x_n)$ is principal.
   Show that $R$ is a PID.

4. Compute with justification the Galois group of the extension $\text{Gal}(\mathbb{Q}(f)/\mathbb{Q})$, where $f(x) = x^4 + x^2 + 1$.

5. Suppose that $K/L$ is a field extension and $M$ is an intermediate subfield. Assume $[K : L] < \infty$ and $\text{Gal}(K/L) = \{e\}$.
   (a) Is it true $\text{Gal}(K/M) = \{e\}$? Justify.
   (b) Is it true $\text{Gal}(M/L) = \{e\}$? Justify.
Math 553 Qualifying Exam

January, 2018  Ron Ji

You must provide necessary arguments to support your claims. You may only use theorems and basic examples proved in the lectures. Solutions must be shortened for simplicity.

1. Let $H$ be a normal subgroup of a group $G$ of index $p$, where $p$ is a prime number. Prove that for any subgroup $K$ of $G$ not contained in $H$, $[K : K \cap H] = p$.

2. Show that there is no simple group of order 1755.

3. Let $\mathbb{Z}[i]$ be the ring of Gaussian integers. Let $I$ be the ideal generated by $7 - 4i$ and $-1 + 8i$.
   (a) Show that $\mathbb{F} = \mathbb{Z}[i]/I$ is a field.
   (b) Determine the characteristic $p$ of $\mathbb{F}$ and the number of elements in $\mathbb{F}$ from part (a).
   (c) Find the irreducible polynomial $f \in \mathbb{Z}_p[x]$ so that the field $\mathbb{F}$ is a splitting field of $f$ over $\mathbb{Z}_p$.

4. Let $R$ be the integral ring $\mathbb{Z}[\sqrt{10}] = \{a + b\sqrt{10} | a, b \in \mathbb{Z}\}$.
   (a) Show that the equation $a + b\sqrt{10}$ is a unit if and only if $a^2 - 10b^2 = 1$.
   (b) Show that 2, 3, and $4 \pm \sqrt{10}$ are irreducibles. (Hint: No square of an integer ends with 2 and 3 in ones place.)
   (c) Show that $4 + \sqrt{10}$ is not a prime.

5. Let $K$ be the splitting field of $f(x) = x^4 - 5$ over $\mathbb{Q}$.
   (a) Determine the degree of the extension $K/\mathbb{Q}$.
   (b) Determine the Galois group $G = \text{Aut}_\mathbb{Q}K$ and identify $G$ as a known group.
   (c) Determine each subgroup of $G$ and its fixed field of the extension $K/\mathbb{Q}$.

6. Let $K/F$ be a finite extension and $E$ is an intermediate field. Suppose $K/E$ and $E/F$ are Galois. Show that $K/F$ is Galois if and only if every $F$-automorphism of $E$ can be extended to an $F$-automorphism of $K$. Find an example that both $K/E$ and $E/F$ are Galois extensions but $K/F$ is not Galois.
(1) a) Prove that every group $G$ of order $24 = 2^3 \cdot 3$ is solvable. (Hint: consider the action of $G$ on its Sylow 2 subgroups.)

b) Prove that every group of order $312 = 2^3 \cdot 3 \cdot 13$ is solvable.

(2) Let $A = \mathbb{Z}/60 \times \mathbb{Z}/60 \times \mathbb{Z}/40$.

a) Find the invariant factor and elementary divisor decompositions of $A$.

b) Find the invariant factor and elementary divisor decompositions of the subgroup of $A$ generated by the elements $a = ([10], [6], [24])$ and $b = ([15], [9], [16])$, where $[n] \in \mathbb{Z}/m\mathbb{Z}$ denotes the coset $n + m\mathbb{Z}$.

(3) Let $R$ be a commutative, unital ring.

a) Prove that the set $N = \{ r \in R : r^n = 0 \text{ for some } n \in \mathbb{N} \}$ is an ideal of $R$.

b) Prove that $N$ is a maximal ideal if and only if every element of $R$ that is not in $N$ is a unit.

(4) a) Show that the ring $\mathbb{Z}[x]/(x^3 - 1)$ is isomorphic to $\mathbb{Z} \times \mathbb{Z}[\zeta_3]$, where $\zeta_3 = -1/2 + (\sqrt{3}/2)i \in \mathbb{C}$, and $\mathbb{Z}[\zeta_3] \subset \mathbb{C}$ is the subring of $\mathbb{C}$ generated by $\zeta_3$.

b) Find all units in the ring $\mathbb{Z}[x]/(x^3 - 1)$.

(5) Let $p$, $q$, and $r$ be prime numbers, and let $\mathbb{F}_{p^n}$ ($n = 1, 2, \ldots$) denote the finite field with $p^n$ elements. Consider the action of the Galois group of the extension $\mathbb{F}_{pqr}/\mathbb{F}_p$ on the elements of $\mathbb{F}_{pqr}$. Find the sizes of the orbits, and the number of orbits of each size.

(6) Let $f(x) \in \mathbb{Q}[x]$ be an irreducible cubic polynomial with three real roots $\alpha, \beta, \gamma \in \mathbb{R}$ such that $\alpha$ is negative and $\beta$ is positive. Prove that the Galois group of the degree 6 polynomial $p(x) = f(x^2)$ is non-abelian.
(1) a) Prove that if \( G \) is a group of order \( 2^2 \cdot 5^2 \cdot 11 \), then \( G \) contains either a normal subgroup of order 11, or a normal subgroup of order \( 2^2 \cdot 5^2 \).

b) Prove that all groups of order \( 2^2 \cdot 5^2 \cdot 11 \) are solvable.

(2) Let \( Z_n = \mathbb{Z}/n\mathbb{Z} \) denote the cyclic group of order \( n \), and for \( a \in \mathbb{Z} \), let \( \overline{a} \) denote its image in \( Z_n \).

Consider the group
\[
A = \mathbb{Z}_{3 \cdot 5^2} \times \mathbb{Z}_{5^2 \cdot 7}
\]
and let \( C \leq A \) be the cyclic subgroup generated by \( (15, 35) \).

a) Find the invariant factor and the elementary divisor decompositions of the quotient group \( A/C \).

b) Do the elements \( (7, 35) \) and \( (35, 7) \) represent the same element in \( A/C \)? Explain your answer.

(3) Let \( K \leq S_7 \) be the subgroup generated by \( \sigma = (1 \ 2)(3 \ 4) \) and \( \tau = (1 \ 3)(2 \ 4) \). Describe the group \( K \), and calculate the number of subgroups in \( S_7 \) that are conjugate to \( K \).

(4) Consider the ring \( R = \mathbb{Z}[\sqrt{-5}] \).

a) Show that the ideal of \( R \) generated by \( 6 + \sqrt{-5} \) is maximal.

b) Let \( I = (41) \) be the ideal of \( R \) generated by \( 41 = 41 + 0\sqrt{-5} \). Show that the quotient ring \( R/I \) is isomorphic to \( \mathbb{Z}/41\mathbb{Z} \times \mathbb{Z}/41\mathbb{Z} \). (The Chinese Remainder Theorem may be helpful here.)

(5) Let \( p(x) \in \mathbb{Q}[x] \) be an irreducible polynomial of degree \( n \), and let \( G \) be the Galois group of \( p(x) \). Prove that if \( G \) is abelian, then \( |G| = n \).

(6) Let \( p(x) = x^6 - 3 \in \mathbb{Q}[x] \), and let \( K \subset \mathbb{C} \) be the splitting field for \( p(x) \).

a) Find a generating set for the \( \text{Gal}(K/\mathbb{Q}) \) (the Galois group of \( p(x) \)), and describe the action of each generator as a permutation of the roots of \( p(x) \).

b) Calculate \( \text{Gal}(K/\mathbb{Q}) \) (it is isomorphic to a familiar group).

c) Prove that there is a unique intermediate subfield \( \mathbb{Q} \subset E \subset K \) satisfying \( [E : \mathbb{Q}] = 4 \), and show that \( E \cap \mathbb{R} = \mathbb{Q}(\sqrt{3}) \).
Problem 1. Let $p$ be a prime number and let $G = \mathbb{Z}_p \times \mathbb{Z}_{p^2}$ be the product of cyclic groups of orders $p$ and $p^2$. Classify the subgroups of $G$ up to isomorphism. Give the number of distinct subgroups of each type.

Problem 2. Let $G$ be a group and let $H \leq G$ be a subgroup of index 2. Is $H$ necessarily a characteristic subgroup?

Problem 3. Let $R$ be a commutative ring. An ideal $I \subset R$ is called irreducible if it is not a non-trivial intersection of two ideals: $J, K \subset R$ are ideals and $I = J \cap K$ implies $I = J$ or $I = K$. True or false (explain!):
   a) Every prime ideal is irreducible.
   b) Every irreducible ideal is prime.

Problem 4. Factorize 2013 into primes over
   a) $\mathbb{Z}$
   b) $\mathbb{Z}[i]$
   c) $\mathbb{Z}[\sqrt{-2}]$

Problem 5. Give an example of a polynomial of degree 6 with Galois group $S_3 \times \mathbb{Z}_2$. Here $S_3$ is the symmetric groups on three elements and $\mathbb{Z}_2$ is the cyclic group of order 2.

Problem 6. Let $\xi = 1 - 2e^{\pi i/7}$. Show that $\xi$ is algebraic over $\mathbb{Q}$ and find the minimal polynomial $m_{\xi,\mathbb{Q}}(x) \in \mathbb{Q}[x]$. 
You must provide necessary arguments to support your claims. You may use any theorems and basic examples from the textbooks but not from homework. Solutions must be shortened for simplicity.

1. (20) Let $A_6$ be the alternating group on six letters.
   (a) Does $A_6$ have a subgroup of order 72? Justify your answer.
   (b) Does $A_6$ have a subgroup of order 45? Justify your answer.

2. (20) If $G$ is a finite group with order $pqr$, where $p < q < r$ are prime numbers. Let $P$, $Q$ and $R$ be Sylow $p$, $q$ and $r$-subgroup, respectively.
   (a) Show that either $P$, $Q$ or $R$ is a normal subgroup.
   (b) If $P$ (or $Q$) is normal in $G$, show that $G/P$ (resp. $G/Q$) has a normal subgroup of order $r$.
   (c) Show that $R$ is a normal subgroup in $G$.

3. (20) Let $\mathbb{Z}[i]$ be the ring of Gaussian integers.
   (a) Show that $F = \mathbb{Z}[i]/(3 + 8i)$ is a field, where $(3 + 8i)$ is the ideal generated by $3 + 8i$.
   (b) Determine the characteristic $p$ and the number of elements in $F$ from part (a).
   (c) Find the irreducible polynomial $f \in \mathbb{Z}_p[x]$ so that the field $F$ is a splitting field of $f$ over $\mathbb{Z}_p$.
   (d) What is the largest degree among all irreducible factors of $x^{p^2} - x$ in $\mathbb{Z}_p[x]$? Why?

4. (20) Let $R$ be a UFD. Let $a$ and $b$ be non-zero-non-unit elements in $R$ such that $a$ is a factor of $b$. Show that there is a natural surjective homomorphism $\pi: R/(b) \rightarrow R/(a)$ which induces a surjection $\pi^\times: (R/(b))^\times \rightarrow (R/(a))^\times$. Here $R^\times$ is the set of units of $R$. (Hint: Chinese Remainder Theorem may be helpful).

5. (20) Let $K = \mathbb{Q}(\sqrt{2}, i)$ and $F = \mathbb{Q}(\sqrt{2})$.
   (a) Show that the extension $\mathbb{Q}(i, \sqrt{2})/\mathbb{Q}(\sqrt{2})$ is a Galois extension.
   (b) Find the order of the Galois group $\text{Aut}_{\mathbb{Q}(\sqrt{2})}\mathbb{Q}(i, \sqrt{2})$.
   (c) Determine the structure of the Galois group $\text{Aut}_{\mathbb{Q}(\sqrt{2})}\mathbb{Q}(i, \sqrt{2})$. 
You must provide necessary arguments to support your claims. You may use any theorems and basic examples from the textbooks but not from homework. Solutions must be shortened for simplicity.

1. (20) Show that a group of order $7007 = 7^2 \times 11 \times 13$ is abelian and find all isomorphism types of this group.

2. (20) Let $G$ be a finitely generated abelian group and $H$ be a subgroup. Let $G_t$ and $H_t$ be the corresponding torsion subgroups of $G$ and $H$, respectively. If $G/G_t$ has rank $n$ and $H/H_t$ has rank $k$, show that $(G/H)/(G/H)_t$ has rank $n - k$.

3. (20) Let $\mathbb{Z}[i]$ be the ring of Gaussian integers. Let $N(a + bi) = a^2 + b^2$ be the norm function on $\mathbb{Z}[i]$.
   (a) Show that $\mathbb{F} = \mathbb{Z}[i]/(2 - 3i)$ is a field, where $(2 - 3i)$ is the ideal generated by $2 - 3i$.
   (b) Determine the number of elements in $\mathbb{F}$ from part (a) and the characteristic $p$ of the field $\mathbb{F}$.

4. (20) Let $R$ be a PID. An ideal $P$ is said primary if whenever $ab \in P$ but $a \not\in P$ imply $b^n \in P$ for some $n$. Show that a nontrivial ideal $P$ is primary if and only if for some $n$, $P = (p^n)$ where $p \in R$ is a prime element. (Don’t forget $R$ is a PID.)

6. (20) Let $\zeta_8 = \frac{\sqrt{2}}{2}(1 + i)$ be the primitive 8th root of unity.
   (a) Show that $\mathbb{Q}(\zeta_8, \sqrt{2}) = \mathbb{Q}(i, \sqrt{2})$ and the extension $\mathbb{Q}(\zeta_8, \sqrt{2})/\mathbb{Q}$ is a Galois extension.
   (b) Find the order of the Galois group $\text{Aut}_{\mathbb{Q}}\mathbb{Q}(\zeta_8, \sqrt{2})$.
   (c) Determine the Galois group $\text{Aut}_{\mathbb{Q}}\mathbb{Q}(\zeta_8, \sqrt{2})$. 

Problem 1. Let $G$ be a finite group of order $7^3 \cdot 31$. Assume that $G$ has a cyclic group of order $7^3$. Show that $G$ is cyclic.

Problem 2. Describe all group homomorphisms $\mathbb{Z}_6 \to \mathbb{Z}_{24}$. In each case describe kernel and image. (Here $\mathbb{Z}_m$ is the cyclic group of order $m$.)

Problem 3. Let $G, H$ be finite groups. Let $K = H \rtimes_\phi G$ be a semidirect product. (Here $\phi : G \to \text{Aut}(H)$ is a homomorphism of groups.)
    
    True or false? Explain your answers!
    a) If $G$ and $H$ are abelian then $K$ is abelian.
    b) If $G$ and $H$ are solvable then $K$ is solvable.
    c) If $G$ and $H$ are nilpotent then $K$ is nilpotent.

Problem 4. An element $x$ of a commutative ring $R$ is called nilpotent if $x^n = 0$ for some $n \in \mathbb{Z}_{\geq 0}$. Let $\text{Nil}(R)$ be the set of all nilpotent elements in ring $R$.
    a) Show $\text{Nil}(R)$ is an ideal.
    b) If $I \subset R$ is an ideal and $\text{Nil}(R/I) = \{0\}$ then $\text{Nil}(R) \subset I$. Is the converse statement true?
    c) Let $R = \mathbb{Z}[x]$ and let $I \subset R$ be the principal ideal generated by polynomial $12(x - 1)x^2(x + 1)^3$. Describe the ideal $\text{Nil}(R/I)$. Is this ideal principal?

Problem 5. Describe the group of units of the ring $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$.

Problem 6. What is the Galois group of the polynomial $p(x) = 3x^4 + 20x^2 + 30 \in \mathbb{Q}[x]$? Describe the splitting field of $p(x)$ and all subfields.
Problem 1. Let $p$ be a prime number and $G = \mathbb{Z}_p \times \mathbb{Z}_{p^2}$ the product of cyclic groups of orders $p$ and $p^2$.

- a) Count the number of subgroups of $G$ of order $p$.
- b) Count the number of subgroups $K \subset G$ such that $G/K$ is isomorphic to $\mathbb{Z}_{p^2}$.
- c) Count the number of subgroups $K \subset G$ such that $G/K$ is isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$.

Problem 2. Let $A_n \subset S_n$ be the alternating group. For which $n$ is $A_n$ a semidirect product of two non-trivial subgroups? Explain.

Problem 3. Let $R$ be a commutative ring. Give the definition of a prime ideal $I \subset R$. Suppose $I$, $J$, $I \cap J$ are all prime ideals of $R$. Show that $I \subset J$ or $J \subset I$.

Problem 4. Let $F_5 = \mathbb{Z}/5\mathbb{Z}$ be the field with 5 elements. Show that the quotients $F_5[x]/(x^2 + 2)$ and $F_5[x]/(x^2 + x + 1)$ are fields.

Construct an explicit isomorphism of fields: $F_5[x]/(x^2 + 2) \to F_5[x]/(x^2 + x + 1)$.

Problem 5. Give a definition of a Galois extension. Let $K \subseteq M \subseteq L$ be fields. True or false? Explain!

- a) If $L : K$ is a Galois extension, then $M : K$ is a Galois extension.
- b) If $L : K$ is a Galois extension, then $L : M$ is a Galois extension.
- c) If $M : K$ and $L : M$ are Galois extensions, then $L : K$ is a Galois extension.

Problem 6. Give a polynomial $p(x) \in \mathbb{Z}[x]$ with Galois group

- a) $\mathbb{Z}_6$.
- b) $\mathbb{Z}_3$. 
Problem 1. (15)

(a) Show that in a domain principal prime ideals are maximal among principal ideals.

(b) Show that if $d \in \mathbb{Z}$ is not a square of an integer, then any non-zero prime ideal (not necessarily principal) in the quadratic domain $\mathbb{Z}[\sqrt{d}]$ is maximal.
Problem 2. (10)
Let $M$ be a maximal ideal in a commutative ring $R$ with identity and $n$ be a positive integer. Show that $R/M^n$ has a unique prime ideal, where $M^n$ is the ideal of $R$ generated by the set 
\[ \{x_1x_2\cdots x_n|x_1, x_2, ..., x_n \in M}\]
Problem 3. (10)
Factor $19 + 4i$ as a product of irreducibles in the ring $\mathbb{Z}[i]$. Justify your answer.
Problem 4. (10)
Let \( f \) be an irreducible polynomial of degree \( n \) over the field \( F \). Let \( g \) be any polynomial of positive degree in \( F[x] \). Show that any irreducible factor of \( f \circ g \) has degree divisible by \( n \).
Problem 5. (15)

Let $\zeta$ be a primitive 7th root of unity in $\mathbb{C}$. Determine the following with proofs.

(a) The galois group $\text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta))$;
(b) All intermediate subfields of the extension $\mathbb{Q}(\zeta)/\mathbb{Q}$. 

Problem 6. (15)
Show that any group $G$ with $|G| = 105$ is solvable.
Problem 7. (20) Let $G$ be a finite abelian group (written multiplicatively) and let $p$ be a prime. Define the subgroups: $G^p = \{a^p|a \in G\}$ and $G_p = \{x \in G|x^p = 1\}$.

(a) Prove that $G/G_p \cong G^p$ and $G/G^p \cong G_p$.

(b) Prove that the number of subgroups of $G$ of order $p$ equals the number of subgroups of $G$ of index $p$. 
Problem 1. (20)
Let $G$ be a finite group and $p$ be a prime number such that $p$ divides the order of $G$. Let $n_p$ be the number of Sylow $p$-subgroups in $G$. If $n_p \not\equiv 1 \pmod{p^2}$, show that there are two Sylow $p$-subgroups $P$ and $Q$ such that $[P : P \cap Q] = p$. (Hint: Consider the action of $P$ on the set of all Sylow $p$-subgroups by conjugation.)
Problem 2. (30)
Let $R$ be a commutative ring with identity. Let $\mathcal{N}$ be the set of all nilpotent elements in $R$. Prove the following:

(a) $\mathcal{N}$ is an ideal of $R$.

(b) $\mathcal{N}$ is contained in the intersection of all prime ideals of $R$.

(c) $\mathcal{N}$ is exactly the intersection of all prime ideals of $R$. (Hint: If not, let $P_0$ be the intersection and $a \in P_0 - \mathcal{N}$. Let $M$ be the partially ordered set consisting of ideals that do not contain any power of $a$. Show that $M$ has a maximal element.)
Problem 3. (30)
Let $K/F$ be a finite Galois extension with Galois group of order $3393 = 3^2 \cdot 13 \cdot 29$. Show that there are intermediate subfields $E_1$, $E_2$ and $E_3$ such that

1. $E_0 = F \subset E_1 \subset E_2 \subset E_3 \subset E_4 = K$, where each containment is proper, and
2. $E_{i+1}/E_i$ is a Galois extension for $i = 0, 1, 2, 3$.

Determine the Galois groups $\{\text{Gal}(E_{i+1}/E_i)|i = 0, 1, 2, 3\}$ as a set.
Problem 4. (20)
Let $p$ be a prime number and $F$ be a finite field of order $p$.

(a) Show that if $a$ is a nonzero element in $F$, then the polynomial $f = x^p - x + a$ is irreducible over $F$. (Hint: If $\alpha$ is a zero of $f$, consider $\alpha + 1$.)

(b) Decide if the splitting fields of $f_1 = x^3 - x + 1$ and $f_2 = x^3 - x - 1$ over $F = \mathbb{Z}_3$ are isomorphic or not. If they are, find an explicit isomorphism between them. If not, explain why.
Problem 1. Let $G$ be a group of order $385 = 5 \cdot 7 \cdot 11$. Show that if it has a normal subgroup of order 5 then it is cyclic. Give an example of a non-commutative group of order 385.

Problem 2. Let $p$ be a prime and let $Z_p$ and $Z_{p^2}$ be the cyclic groups of orders $p$ and $p^2$ respectively. Let $G = \text{Aut}(Z_p \times Z_{p^2})$ be the group of automorphisms of the direct product. Show that $G$ is non-abelian and find the order of $G$.

Problem 3. Let $S_3$ be the symmetric group on three elements and let $R = \mathbb{Z}S_3$ be the group ring of $S_3$. Describe the center of ring $R$.

Problem 4. Is the ideal of $\mathbb{Z}[x, y]$ generated by $x^2 + xy + y^2$ and $x + y + x^2 + y^2$ prime?

Problem 5. Describe explicitly a finite field $F$ with 9 elements. Find a generator of the multiplicative group $F^\times$.

Problem 6. Describe the splitting field $K$ of $p(x) = x^4 - 18x^2 + 25$ over $\mathbb{Q}$. Identify the Galois group. Describe all subfields of $K$. 
**Problem 1.** Describe all Sylow subgroups of the symmetric group of permutations on four symbols $S_4$ explicitly.

Describe the 2-Sylow subgroup by generators and relations.

**Problem 2.** How many elements of order 75 are in the group $\mathbb{Z}_{50} \times \mathbb{Z}_{15} \times \mathbb{Z}_{18} \times \mathbb{Z}_7$? Here $\mathbb{Z}_s$ denotes the cyclic group of order $s$.

**Problem 3.** Let $G$ be a finite group of odd order. Let $G$ act on the set $\{1, 2, 3\}$. Show that stabilizer subgroups of elements 1, 2, and 3 are all isomorphic.

**Problem 4.** Factor the polynomial $x^3 - 10x + 4$ into a product of irreducible polynomials over each of the fields $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{2}, \sqrt[3]{2}]$, $\mathbb{Z}/11\mathbb{Z}$, $\mathbb{Z}/13\mathbb{Z}$.

**Problem 5.** Let $R$ be a ring and $N \subset R$ a subset. Define the radical of $N$ by the formula

$$r(N) = \{a \in R \mid \text{there exists } n \geq 1, \text{ such that } a^n \in I\}.$$ 

Let $I, J \subset R$ be ideals. Show $r(IJ) = r(I) \cap r(J) = r(I \cap J)$.

**Problem 6.** Let $f(x) = x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$. Describe the splitting field $K$ of $f(x)$ and the Galois group $G$ of $f(x)$. Describe the subgroups of $G$ and the corresponding subfields of $K$. 
You must provide detailed reasoning to support your claims. You may use any theorems (but not examples nor exercises) in the textbook to support your arguments. However, if a problem is itself part of a theorem in the textbook, you must provide proofs.

1. (20) Prove or disprove that there exists a finite group \( G \) with a proper subgroup \( H \) such that \( G = \cup_{g \in G} gHg^{-1} \).

2. (20) Let \( \mathbb{Q} \) be the field of all rational numbers and \( \bar{\mathbb{Q}} \) be the set of all algebraic numbers over \( \mathbb{Q} \). Prove the following.
   (a) \( \bar{\mathbb{Q}} \) is a field.
   (b) \( \bar{\mathbb{Q}} \) has no proper algebraic extensions.

3. (20) Let \( f(x) = x^3 + 3 \in \mathbb{Q}[x] \).
   (a) Determine the Galois group of \( f \) over \( \mathbb{Q} \).
   (b) Show that the splitting field \( \mathbb{Q}_f \) of \( f \) over \( \mathbb{Q} \) is a simple extension by finding an element \( \alpha \) in \( \mathbb{Q}_f \) such that \( \mathbb{Q}_f = \mathbb{Q}[\alpha] \).

4. (20) Factor \( 3 - 11i \) as a product of irreducibles in the ring \( \mathbb{Z}[i] \).

5. (20) (a) Let \( G \) be a group of order 504.
   (a) Prove that \( G \) is not isomorphic to any subgroup of the alternating group \( A_7 \).
   (b) If \( G \) is simple, determine the number of Sylow 3-subgroups.
Math 553 Qualifying Exam

January, 2010

Ron Ji

You must provide detailed reasoning to support your claims. You may use any theorems (but not examples nor exercises) in the textbook to support your arguments. However, if a problem is itself part of a theorem in the textbook, you must provide proofs.

1. (10) Prove that any group of order 30 has a normal subgroup of order 15.

2. (10) Let \( P \) be a Sylow \( p \)-subgroup of a finite group \( G \). If a subgroup \( H \) of \( G \) contains \( N_G(P) \), show that \([ G : H ] \equiv 1 \pmod{p}\).

3. (20) Let \( R \) be an integral domain with quotient field \( F \). Let \( f \) be a monic polynomial in \( R[x] \) of degree \( n > 1 \). Assume that \( f = gh \) for some monic polynomials \( g \) and \( h \) in \( F[x] \) of smaller degree than \( f \). Prove that if \( R \) is a UFD, then \( g \) and \( h \) must be in \( R[x] \). Deduce that \( \mathbb{Z}[\sqrt{5}] \) is not a UFD.

4. (35) Let \( R \) be a commutative ring with identity. Let \( N_R \) be the set of all nilpotent elements in \( R \). Show that
   a) \( N_R \) is an ideal of \( R \);
   b) \( N_R \) is contained in every prime ideal in \( R \);
   c)* (Optional) \( N_R \) is the intersection of all prime ideals in \( R \);
   d) \( R \) has a unique prime ideal if and only if every element in \( R \) is either nilpotent or a unit.
   (Hint: You may use the result in c.).

5. (25) Let \( \sigma : F \rightarrow F' \) be an isomorphism of fields. Let \( f = \sum_{i=0}^{n} a_i x^i \) be an irreducible polynomial in \( F[x] \) and let \( f^\sigma = \sum_{i=0}^{n} \sigma(a_i)x^i \). Let \( E \) be a splitting field of \( f \) over \( F \) and \( E' \) be a splitting field of \( f^\sigma \) over \( F' \). Show that
   (1) \( f^\sigma \) is irreducible in \( F'[x] \);
   (2) There is an isomorphism \( \psi : E \rightarrow E' \) such that \( \psi|_F = \sigma \);
   (3) The Galois groups \( \text{Gal}(E/F) \) and \( \text{Gal}(E'/F') \) are isomorphic.
Math 553 Qualifying Exam

Fall, 2010

Ron Ji

In this test, e denotes the identity element of a group; |g| denotes the order of the group element g; |S| denotes the cardinality of the set S; K/F denotes the field extension K of F.

Even if you may not be able to prove certain parts, you may still use them to prove other statements following them.

1. (25) Let G be a finite group of order 105. Let $P_3$, $P_5$ and $P_7$ be the Sylow 3-subgroup, Sylow 5-subgroup and Sylow 7-subgroup, respectively, of G. Prove the following.

   (a) $P_7$ is normal in G.

   (b) $H = P_3 P_7$ is a subgroup of G and is isomorphic to $P_3 \times P_7$.

   (c) The subgroup $H = P_5 P_7$ is a normal subgroup of G.

   (d) If $P'_5$ is another Sylow 5-subgroup of G, then $P'_5 P_7 = P_5 P_7$.

   (e) $P_5$ is normal in G.
2. (20) Let $G$ be a finite group of order $n$. Suppose that $n = p_1^{a_1}p_2^{a_2} \ldots p_k^{a_k}$, where $p_i$’s are distinct prime numbers and $a_i$’s are natural numbers. Let $S_m = \{g \in G | g^m = e\}$. If $|S_m| \leq m$ for $m = p_i^{t_i}$, where $i = 1, 2, ..., k$ and $t_i \leq a_i$, then prove the following.

(a) Each Sylow $p_i$-subgroup $P_i$ of $G$ is normal.

(b) $G$ is isomorphic to the direct product of the Sylow $p_i$ subgroups of $G$, for $i = 1, 2, ..., k$.

(c) Each Sylow $p_i$-subgroup of $G$ is cyclic.

(d) $G$ is cyclic.
3. (20) Let $R[x]$ be the polynomial ring over a commutative ring $R$ with identity. Prove the following.

(a) $R[x]$ is an integral domain if and only if $R$ is integral.
(b) $R[x]$ is a Euclidean domain if and only if $R$ is a field.
(c) $R[x]$ has a unit not contained in $R$ if $R$ has a nilpotent element.
4. (20) Let $\mathbb{Z}[i]$ be the ring of Gaussian integers. Let $N(a + bi) = a^2 + b^2$ be the norm function on $\mathbb{Z}[i]$.

(a) Prove or disprove that every irreducible element in $\mathbb{Z}[i]$ must have the norm a prime number.

(b) Show that for any nonzero proper ideal $I$ of $\mathbb{Z}[i]$, the quotient ring $\mathbb{Z}[i]/I$ is finite.

(c) Suppose that $I$ is the principal ideal generated by $a + bi \in \mathbb{Z}[i]$ such that $a^2 + b^2 = p$ is an odd prime number. Show that $\mathbb{F} = \mathbb{Z}[i]/I$ is a finite field.

(d) Determine the number of elements in $\mathbb{F}$ from part (c).
5. (30) Let $K$ be a field of characteristic 0. Let $K(x) = \{ \frac{f}{g} | f, g \in K[x], g \neq 0 \}$ be the quotient field of $K[x]$. Prove the following.

(1) If $E$ is an intermediate field of the extension $K(x)$ by $K$ and $E \neq K$. Show that $[K(x) : E]$ is finite. (Hint: Let $f/g$ be an element in $E$ but not in $K$. Assume that $f, g$ are relatively prime, and $\varphi(y) = (f/g)g(y) - f(y) \in K[f/g][y]$. Show that $\varphi$ is irreducible.)

(2) There are infinitely many $K$-automorphisms of $K(x)$.

(3) $K(x)/K$ is an infinite Galois extension of $K$. (Hint: Consider the fixed field of the group $Gal(K(x)/K)$.)
Math 553 Qualifying Exam

Jan. 5, 2009

Ron Ji

You may use any theorems in the textbook but you must provide a complete argument for each problem you prove.

1. (15 points) Let $P$ be a Sylow $p$-subgroup of a finite group $G$ and $H$ be any subgroup of $G$. Show that there is an element $g$ in $G$ such that $gP g^{-1} \cap H$ is a Sylow $p$-subgroup of $H$. Show also by an example that $P \cap H$ is not necessarily a Sylow $p$-subgroup.

2. (10 points) Let $G$ be a finite abelian group with $|G| = n$. Let $d$ be a positive divisor of $n$. Show that the number of elements of $G$ having order $d$ is a multiple of $\phi(d)$, where $\phi$ is the Euler function.

3. (a) (5 points) Let $G = S_3$ be the symmetric group on the set $\{1, 2, 3\}$. Show that the center of the group ring $\mathbb{Z}G$ consists of elements of the form $aK_0 + bK_1 + cK_2$, where $a, b, c$ are integers, $K_0$ is the identity element in $G$, $K_1 = (1 2) + (1 3) + (2 3)$ and $K_2 = (1 2 3) + (1 3 2)$.

(b) (5 points) Show that both $K_1$ and $K_2$ are zero divisors in $\mathbb{Z}G$ but not $K_0$.

(c) (5 points) In general, show that if $G$ is a nontrivial finite group, then the integral group ring $\mathbb{Z}G$ always has a zero divisor.

4. a) (10 points) Let $q \in \mathbb{Z}$ be a prime number such that $q \equiv 3 \pmod{4}$. Show that $q$ is irreducible in $\mathbb{Z}[i]$ and $\mathbb{Z}[i]/(q)$ is isomorphic to a field of $q^2$ elements.

b) (10 points) Show that if a prime $p \equiv 1 \pmod{4}$, then $p$ is a product of two irreducible elements $\pi_1$ and $\pi_2$ in $\mathbb{Z}[i]$ and $\mathbb{Z}[i]/(p) \cong \mathbb{Z}[i]/(\pi_1) \times \mathbb{Z}[i]/(\pi_2)$. (You may use the fact that $p = a^2 + b^2$ for some integers $a$ and $b$.)

5. (10 points) Let $F$ be a field. If the least prime factor of $[F(\alpha) : F]$ is $p$, then the degrees of the minimal polynomials of $\alpha^k$ for $k = 1, 2, \ldots, p-1$ over $F$ are all equal.

6. (15 points) Let $f$ be an irreducible polynomial of degree greater than 1 (not necessarily separable) over a field $F$. Let $F_f$ be the splitting field of $f$ over $F$ and $E$ be an intermediate subfield containing at least one zero of $f$. If for any $\sigma \in \text{Aut}_F F_f$, $\sigma|_E : E \longrightarrow E$, then $E = F_f$.

7. (15 points) Show that the polynomial $x^3 + 2$ is irreducible over $\mathbb{Q}[\zeta]$, where $\zeta$ is the primitive cubic root of unity in $\mathbb{C}$. Find the degree $[Q_f : \mathbb{Q}]$ of the extension $Q_f/\mathbb{Q}$ and determine the Galois group $\text{Aut}_{\mathbb{Q}} Q_f$, where $Q_f$ is the splitting field of $f$ over $\mathbb{Q}$. 
1. (10) Let $G$ be a finite group with proper subgroups $H$, $K$ and $N$. Show that if $N$ is normal and $G = HKN$, then $G = NKH$.

2. (15) Let $G$ be a finite group with a proper normal subgroup $H$. If $P$ is a Sylow $p$-subgroup of $H$, then $G = HN_G(P)$ and $[G : H]$ divides $|N_G(P)|$.

3. (10) Show that the center of a group $G$ of order 231 contains its Sylow 11-subgroup. (Hint: You may consider a possible action of $G$ on its Sylow 11-subgroup.)

4. (20) (a) Determine if $4x^2y^2 + 2xy^2 - 4x^2y + xy + 4x - 1$ is irreducible or not in the ring $\mathbb{Z}[x,y]$.
   (b) Determine if $f(x) = 5x^4 + 6x^2 + 6x - 27$ is irreducible or not in the ring $\mathbb{Z}[x]$.

5. (20) Let $\pi$ be an irreducible element in $\mathbb{Z}[i]$. Let $(\pi)$ be the ideal of $\mathbb{Z}[i]$ generated by $\pi$ and $(\pi) \cap \mathbb{Z} = p\mathbb{Z}$, where $p$ is some positive integer. Show that
   (1) $p$ is a prime number.
   (2) Either $p$ is irreducible in $\mathbb{Z}[i]$ or $p$ is a product of exactly two irreducible elements in $\mathbb{Z}[i]$.
   (3) If $p$ is a product of two irreducible elements in $\mathbb{Z}[i]$, then $p$ is a sum of two squares of integers.
   (4) If $p \equiv 3 \text{(mod 4)}$, then $p$ must be irreducible in $\mathbb{Z}[i]$.

6. (20) Let $f(x) = x^p - x + a$ be in $\mathbb{Z}_p[x]$, where $a \in \mathbb{Z}_p$ and $a \neq 0$. Show that
   (1) $f$ is separable over $\mathbb{Z}_p$. (Hint: if $\alpha$ is a root of $f$ in an extension field, then $\alpha + b$ is also a root of $f$ for any $b \in \mathbb{Z}_p$.)
   (2) If $E$ is a splitting field of $f$ over $\mathbb{Z}_p$ and $\alpha$ is a zero of $f$ in $E$, then $E = \mathbb{Z}_p(\alpha)$.
   (3) $Gal(E/\mathbb{Z}_p) \cong \mathbb{Z}_p$.
   (4) $f$ is irreducible over $\mathbb{Z}_p$ if and only if $a \neq 0 \in \mathbb{Z}_p$.

7. (10) Determine the Galois group of the polynomial $f(x) = x^3 - 3$ over $\mathbb{Q}$. 

Any statement must be proved in complete details.
Problem 1. Let $G$ be a group acting on a finite set $A$. Let $\mathbb{R}(A) = \{ f : A \to \mathbb{R} \}$ be the set of all real-valued functions on $A$. Show that the formula $(gf)(x) = f(g^{-1}x)$ defines an action of the group $G$ on $\mathbb{R}(A)$ and that the kernels of actions of $G$ on $A$ and $R(A)$ coincide.

Problem 2. Let $G$ be a group of order $3 \cdot 5 \cdot 11$. Show that the center of $G$ contains a subgroup of order 11.

Problem 3. Let $p$ be an odd prime. Show that $x^2 + 1$ is reducible over $\mathbb{Z}/p\mathbb{Z}$ if and only if $p - 1$ is not divisible by 4.

Problem 4. How many units and how many ideals does the ring $\mathbb{Z}/60\mathbb{Z}$ have?

Problem 5. For what $n$ is the ring $\mathbb{Z}/n\mathbb{Z}$ a direct sum of fields?

Problem 6. For a prime $p$, let $F_p$ be the field of order $p$. Consider the set

$$M_p = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} , \ a, b \in F_p \right\}$$

with the standard matrix operations. How that $M_{11}$ is a field but $M_{13}$ is not.

Problem 7. Let $F_7$ be the field of order 7. Find all $a \in F_7$ such that $F_7[x]/(x^3 + ax + 1)$ is a field. What is the order of that new field(s)?

Problem 8. Describe the splitting field of the polynomial $p(x) = x^4 - 10x^2 + 5$ over $\mathbb{Q}$ and compute the corresponding Galois group.
Problem 1. Let $G$ be a cyclic group of order 2008 with generator $a$. Find all $b \in G$ such that $G/\langle b \rangle$ is isomorphic to $\langle a^{100} \rangle$. (Here $\langle c \rangle$ denotes the subgroup of $G$ generated by $c \in G$.)

Problem 2. Let $G$ be a group of order $2^2 \cdot 3 \cdot 11$. Show that $G$ is not simple.

Problem 3. Let $G = SL(2, \mathbb{Z})$ be the group of $2 \times 2$ matrices with integer entries and determinant 1. Let $H \subset \mathbb{C}$ be the upper half plane of complex numbers, $H = \{ z \in \mathbb{C} \mid \text{Im } z > 0 \}$. Show that the formula
\[
\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az + b}{cz + d}
\]
defines an action of $G$ on $H$ and show that all orbits are infinite.

Problem 4. Let $R$ be a commutative ring with ideals $I$ and $J$. Assume that $IJ$ is a principal ideal. Show that both $I$ and $J$ are finitely generated.

Problem 5. Show that the ring $R = \{ a + b\sqrt{-2}, a, b \in \mathbb{Z} \}$ is a Euclidean domain with the norm function $N(a + b\sqrt{-2}) = a^2 + 2b^2$ and therefore a unique factorization domain. Write the prime decomposition of 6 in $R$.

Problem 6. Compute the Galois group of the polynomial $p(x) = x^4 - 14x^2 + 9$ over $\mathbb{Q}$. List all the subgroups of the Galois group and the corresponding intermediate fields.

Problem 7. Describe explicitly an injective homomorphism from the symmetric group $S_3$ to the group $GL(2, \mathbb{R})$ of $2 \times 2$ invertible matrices with real coefficients. (Hint: $S_3$ acts in $\mathbb{R}^3$ by permuting the coordinates of the vectors and the 2-dimensional plane $x + y + z = 0$ is invariant under this action.)

Problem 8. Let $G = \mathbb{Z} + \mathbb{Z}$ be a free abelian group of rank 2 with generators $x$ and $y$. Let $H \subset G$ be the subgroup generated by two elements $2x + 2y$ and $x + 3y$. Describe the groups $H$ and $G/H$. 
1. (10) Show that a group of order 1575 is a solvable group.

2. (10) Let $G$ be a finite abelian $p$-group for some prime number $p$. If $a \in G$ is an element of maximal order among all elements in $G$, without using the fundamental theorem of finitely generated abelian groups show that there exists a subgroup $H$ of $G$ such that $G \cong H \times (a)$, where $(a)$ is the cyclic subgroup of $G$ generated by $a$.

3. (10) Show that if $d \in \mathbb{Z}$ is not a square of an integer, then any non-zero prime ideal in the quadratic domain $\mathbb{Z}[\sqrt{d}]$ is maximal. (Hint: Show first that there is a non-zero integer in the prime ideal.)

4. Let $R$ be a non-zero commutative ring with identity.
   a) (10) Show that the polynomial ring $R[x]$ is a PID if and only if $R$ is a field.
   b) (10) Show that the polynomial ring $R[x, y]$ is never a PID.

5. a) (10) Find a generator of the ideal $I$ in $\mathbb{Z}_{17}[x]$ that is generated by $2x^2 - 11x - 6$ and $2x^3 + 11x^2 + 12x + 1$.
   b) (10) Let $I$ be the ideal in $\mathbb{Z}[x]$ that is generated by 5 and $x^2 + 6x - 2$. Show that $I$ is not a prime ideal but is contained in a prime ideal. Construct explicitly such a prime ideal.

6. a) (10) Determine the irreducible polynomial $f_\alpha$ of the element $\alpha = \sqrt{6} + \sqrt{7}$ over the field of rational numbers $\mathbb{Q}$.
   b) (10) Find the Galois group $\text{Gal}_{\mathbb{Q}} f_\alpha$.
   c) (10) Determine the Galois correspondence between the set of intermediate fields of the extension $\mathbb{Q}_{f_\alpha}/\mathbb{Q}$ and the set of subgroups of $\text{Gal}_{\mathbb{Q}} f_\alpha$. Here $\mathbb{Q}_{f_\alpha}$ is the splitting field of $f_\alpha$ over $\mathbb{Q}$.

7. a) (10) Let $K$ be a finite Galois extension over the field $F$. $f \in F[x]$ is an irreducible polynomial of degree $p$, where $p$ is a prime number. Show that $f$ either splits as a product of linear factors or is irreducible in $K[x]$.
   b) (10) Show that $x^5 + x + 1$ is irreducible in $\mathbb{F}_4[x]$, where $\mathbb{F}_4$ is the field of 4 elements.
Do any 10 problems. You must provide detailed reasoning to support your claims. You may use any theorems in the textbook (except those asked in the test) to support your arguments.

1. (10) Show that a group of order 1573 is a solvable group.

2. (10) Show that if \( n_p \not\equiv 1 \pmod{p^2} \) then there exist distinct Sylow \( p \)-subgroups \( P \) and \( Q \) of \( G \) such that \([P : P \cap Q] = [Q : P \cap Q] = p\), where \( n_p \) is the number of \( p \)-Sylow subgroups in \( G \). (Hint: Recall the proof of Sylow’s Theorems.)

3. (10) Let \( P \) be a \( p \)-Sylow subgroup in \( G \). Prove that two elements in the center of \( P \) are conjugate in \( G \) if and only if they are conjugate in \( N_G(P) \), the normalizers of \( P \) in \( G \).

4. (10) Let \( G \) be a group of order \( n \) and \( k \) be a positive integer relatively prime to \( n \). Show that the map \( x \rightarrow x^k \) is surjective.

5. (10) Let \( k \) be a positive integer and let \( A \) be the free abelian group of rank \( n \) written additively. Prove that \( A/kA \) is isomorphic to the direct product of \( n \) copies of \( \mathbb{Z}/k\mathbb{Z} \). (Here: \( kA = \{ka | a \in A\} \)).

6. (10) Determine all ring homomorphisms from \( \mathbb{Z} \times \mathbb{Z}_n \) to \( \mathbb{Z}_m \), where \( n > 1 \) and \( m > 1 \) are positive integers.

7. (10) Let \( m \) and \( n \) be positive integers with \( n \) dividing \( m \). Prove that the natural surjective ring projection \( \mathbb{Z}_m \longrightarrow \mathbb{Z}_n \) is also surjective on the units: \( \mathbb{Z}_m^\times \longrightarrow \mathbb{Z}_n^\times \).

8. (10) Find a generator for the ideal generated by \( 7 + 4i \) and \( -5 + 10i \) in the ring \( \mathbb{Z}[i] \).

9. (10) Determine if the polynomial \( x^5 + 3x^4 - 6x + 6 \) is irreducible or not in the polynomial ring \( \mathbb{Q}[i][x] \) over the field \( \mathbb{Q}[i] \).

10. (10) Determine the splitting field and the degree of the extension of the polynomial \( f = x^6 - 4 \) over \( \mathbb{Q} \). Justify your answer.

11. (10) Determine the Galois group of \( f \) in the previous problem over \( \mathbb{Q} \).

12. (10) The algebraic closure of a field \( F \) is defined to be an extension field \( \bar{F} \) containing \( F \) such that any polynomial over \( F \) splits over \( \bar{F} \). Show that the algebraic closure of \( \bar{F} \) is \( \bar{F} \).