MATH 553, Fall 2015
Final Exam
Solutions

Instructions: Give a complete solution to each problem. You may use any result from class, the book, or homework **except** the statement you are asked to prove (or whose proof depends on the statement you are trying to prove). Be sure to justify your statements.

1. **(15 points)** Let G be a finite non-abelian group, and let $Z(G)$ be the center of G. Prove $|Z(G)| \le \dfrac{|G|}{4}$.

   Solution: Suppose $|Z(G)| > \dfrac{|G|}{4}$. Then

$$|G/Z(G)| = \frac{|G|}{|Z(G)|} < \frac{|G|}{\frac{|G|}{4}} = 4.$$

   So $|G/Z(G)| = 1, 2,$ or 3. But any group of those orders is cyclic. If $G/Z(G)$ is cyclic then G is abelian, contradicting our assumption. So $|Z(G)| \le \dfrac{|G|}{4}$. $\square$

2. Let

$$G = SL_2(\mathbb{Z}/5\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in \mathbb{Z}/5\mathbb{Z}, \text{ and } ad - bc = 1 \pmod 5 \right\}.$$

   (a) **(15 Points)** Show $|G| = 120$.

   (b) **(8 points)** Show $N = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \middle| b \in \mathbb{Z}/5\mathbb{Z} \right\}$ is a Sylow 5-subgroup of G.

   (c) **(12 points)** Find the number of Sylow 5–subgroups of G.

   Solution

   (a) First suppose $c = 0$, so $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$, with $ad = 1$. So $d = a^{-1}$, and b is arbitrary. Thus, there are 4 choices for a, 5 choices for b, so there are 20 elements with $c = 0$. Now, suppose $c \neq 0$. Since $ad - bc = 1$, $b = (ad-1)/c$. So there are 4 choices for c, and 5 each for a and d, and then b is fixed. Thus, there are 100 elements with $c \neq 0$. Thus, $|G| = 120$.

   (b) Note $120 = 2^3 \cdot 3 \cdot 5$, so a Sylow 5–subgroup has order 5. Note $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix}$, so

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -c \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b-c \\ 0 & 1 \end{pmatrix} \in N.$$

So, N is a subgroup, and since there are 5 choices for b, we have $|N| = 5$. Hence N is a Sylow 5–subgroup.

(c) Let n_5 be the number of Sylow 5 subgroups. By Sylow's Theorems we have $n_5 \equiv 1 \mod 5$, and $n_5 \mid (|G|/|N|) = 120/5 = 24$. So $n_5 = 1$, or 6. Note N is one Sylow 5–subgroup, and $\bar{N} = \left\{ \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} \right\}$ is another, so $n_5 \neq 1$, and hence $n_5 = 6$.

Alternative 1: Note that N is not normal by showing one $g \in G$ and one $n \in N$ with $gng^{-1} \notin N$, so that $n_5 \neq 1$. For example $g = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $n = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ gives $gng^{-1} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, so $n_5 = 6$.

Alternative 2:

We let $Syl_5(G) = \{N = P_1, P_2, \ldots, P_r\}$. be the set of Sylow 5–subgroups. by Sylow's Theorems, we know all Sylow 5–subgroups are conjugate in G. So let G act on $Syl_5(G)$ by conjugation. This is an action with one orbit, and by the Orbit-Stabilizer Theorem $r = [G : N_G(N)]$, where $N_G(N)$ is the normalizer of N in G. We have

$$N_G(N) = \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} | a \in (\mathbb{Z}/5\mathbb{Z})^{\times}, b \in \mathbb{Z}/5\mathbb{Z} \right\}.$$

In (a) we saw the order of this subgroup is 20. Thus, $r = 120/20 = 6$. $\square$

3. **(25 points)** Suppose R is a UFD and F is the quotient field of R. Let $f(x) \in R[x]$, and suppose $f(x)$ factors as a product of lower degree polynomials in $F[x]$. Show $f(x)$ factors as a product of lower degree polynomials in $R[x]$.

Solution:

Suppose $f(x) = P(x)Q(x)$ in $F[x]$, with $P(x)$ and $Q(x)$ both of lower degree. Since F is the quotient field of R, the coefficients of $P(x)$ and $Q(x)$ are all of the form $\frac{a}{b}$, with $a, b \in R, b \neq 0$. Now, we can find a common denominator of each of the factors, and multiplying through by these we get an equation

$$df(x) = p_0(x)q_0(x) \tag{1}$$

in $R[x]$, with $p_0(x)$ and $q_0(x)$ of lower degree in $R[x]$. If $d \in R^{\times}$, then $f(x) = (d^{-1}p_0(x))q_0(x)$, with $d^{-1}p_0(x)$ and $q_0(x) \in R[x]$ of lower degree. Now, suppose $d \notin R^{\times}$, and let $d = c_1 c_2 \cdots c_r$, be a factorization with each c_i irreducible. Since c_i is irreducible, (c_i) is a prime ideal in R for each i, and thus $(c_i)R[x]$ is prime in $R[x]$. Now, reduce (1) modulo c_1 and get $0 = \overline{p_0(x)}\,\overline{q_0(x)}$ in $R[x]/(c_1)$, which is an integral domain. Thus either $p_0(x) \in (c_1)$ or $q_0(x) \in (c_1)$. So c_1 divides all the coefficients of one of the factors on the right hand side of (1), and we can cancel c_1

from that factor. We get $c_2c_3\dots c_r f(x) = p_1(x)q_1(x)$ in $R[x]$. Now repeating this process we see each c_i divides one of the factors on the right hand side, so we get $f(x) = p_r(x)q_r(x)$ in $R[x]$ with $p_r(x)$ and $q_r(x)$ of lower degree. $\square$

4. **(12 points each)** Let R be a commutative ring. Recall an element $a \in R$ is **nilpotent** if $a^n = 0$ for some $n \geq 1$. Let $I = \{a \in R | a \text{ is nilpotent}\}$.

   (a) Show I is an ideal. (Hint: To show I is an additive subgroup, show if $x, y \in I$ there is an $N > 0$ so that $(x-y)^N = 0$ using the binomial expansion of $(x-y)^N$.)

   (b) Show I is contained in any prime ideal of R.

   Solution:

   (a) Let $x, y \in I$, and suppose $x^n = 0$, and $y^m = 0$, with $n, m \geq 1$. Let $N = m+n$. Then
   $$(x-y)^N = \sum_{k=0}^{N} x^{N-k}(-y)^k = \sum_{k=0}^{N} (-1)^k x^{N-k} y^k.$$
   If $k < m$, then $N - k > n$, so in each term in the sum either $x^{N-k} = 0$, or $y^k = 0$, and hence the sum is zero. Thus, $x - y \in I$, By the subgroup test I is an additive subgroup of R. Now, if $a \in I$ $r \in R$, then $(ra)^n = r^n a^n$. So if we choose $n \geq 1$ with $a^n = 0$, then $(ra)^n = r^n 0 = 0$, so $ra \in I$. Thus I is an idea, as claimed.

   (b) Let P be a prime ideal, suppose $a \in I$, and $a^n = 0$. If $a \notin P$, then $a + P = \bar{a} \neq \bar{0}$ in R/P. But, since P is prime,R/P is an integral domain, and $\bar{a}^n = \overline{a^n} = \bar{0}$, which would make a a zero divisor. This is a contradiction, and hence $a \in P$, so $I \subset P$. $\square$

5. Let $\alpha \in \mathbb{C}$ be algebraic over $\mathbb{Q}$, and let $f(x) \in \mathbb{Q}[x]$ be its minimal polynomial. Let $\sqrt{\alpha}$ be a square root of α, and let $g(x) \in \mathbb{Q}[x]$ be its minimal polynomial.

   (a) **(8 points)** Show $\deg f(x)$ divides $\deg g(x)$.

   (b) **(18 points)** Show $\sqrt{\alpha} \in \mathbb{Q}(\alpha)$ if and only if $f(x^2)$ is reducible in $\mathbb{Q}[x]$.

   Solution:

   (a) We know if β has minimal polynomial $h(x) \in \mathbb{Q}[x]$, then $[\mathbb{Q}(\beta) : \mathbb{Q}] = \deg h(x)$. Note $\alpha = (\sqrt{\alpha})^2 \in \mathbb{Q}(\sqrt{\alpha})$, so we have $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset \mathbb{Q}(\sqrt{\alpha})$. So,
   $$\deg g(x) = [\mathbb{Q}(\sqrt{\alpha}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{\alpha})\mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = [Q(\sqrt{\alpha}) : \mathbb{Q}(\alpha)] \deg f(x),$$
   and therefore $\deg f(x) | \deg g(x)$.

(b) Let $h(x) = f(x^2)$. Note $\deg h(x) = 2 \cdot \deg f(x)$. Further, $h(\sqrt{\alpha}) = f(\alpha) = 0$, so, since $g(x)$ is the minimal polynomial of $\sqrt{\alpha}$, $g(x)|h(x)$. If $\sqrt{\alpha} \in \mathbb{Q}(\alpha)$, then $Q(\alpha) \supset \mathbb{Q}(\sqrt{\alpha}) \supset \mathbb{Q}(\alpha)$, so $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{\alpha})$, and therefore $\deg g(x) = \deg f(x)$. Since $\deg h(x) = 2 \cdot \deg f(x) = 2 \cdot \deg g(x) > \deg g(x)$, we see $h(x)$ must be reducible. On the other hand, if $h(x)$ is reducible, then $\deg h(x) > \deg g(x)$, and hence $2 \deg f(x) > \deg g(x)$. Since $\sqrt{\alpha}$ satisfies $x^2 - \alpha \in \mathbb{Q}(\alpha)[x]$, we see $[\mathbb{Q}(\sqrt{\alpha}) : \mathbb{Q}] \leq 2$. So, $[Q(\sqrt{\alpha} : \mathbb{Q}] = \deg g(x) < \deg h(x) = 2 \deg f(x) = 2[\mathbb{Q}(\alpha) : \mathbb{Q}]$, and hence $\deg g(x) = \deg f(x)$, and $\sqrt{\alpha} \in \mathbb{Q}(\alpha)$. $\square$

6. Let $f(x) = x^6 + 3 \in \mathbb{Q}[x]$.

a) **(12 points)** Let α be a root of $f(x)$. Prove $\frac{\alpha^3+1}{2}$ is a primitive 6^{th} root of unity.

b) **(18 points)** Determine the Galois group of $f(x)$ over $\mathbb{Q}$.

Solution:

(a) Note $\alpha^6 = -3$, so $\alpha^3 = \pm\sqrt{-3} = \pm i\sqrt{3}$. Thus $\dfrac{\alpha^3 + 1}{2} = \dfrac{1 \pm i\sqrt{3}}{2} = e^{\pi i/3}$, or $e^{5\pi i/3}$, which are the two primitive 6–th roots of unity.

(b) Note, by Eisenstein's Criteria, with $p = 3$, we have $f(x)$ is irreducible. Let $\zeta_6 = e^{\pi i/3}$. By (a), $\mathbb{Q}(\zeta_6) \subset \mathbb{Q}(\alpha)$. Moreover, $\left\{\alpha\zeta_6^j\right\}_{j=0}^5$ are the 6 roots of $f(x)$, and hence $\mathbb{Q}(\alpha)$ is a splitting field of $f(x)$. Now for each j we define σ_j by $\sigma_j(\alpha) = \alpha\zeta_6^j$. Note this uniquely determines σ_j, $\sigma_{j+k} = \sigma_j\sigma_k$, and clearly $\sigma_j = 1$ if and only if $j = 0 \mod 6$, so $j \mapsto \sigma_j$ is an isomorphism form $\mathbb{Z}/6\mathbb{Z}$ to $G = \mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$.

Alternatively, Since $f(x)$ is irreducible $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 6 = |G|$, we know G is a transitive subgroup of order 6 in S_6, and only $\mathbb{Z}/6\mathbb{Z}$ is such a group. $\square$

7. **(15 points each)** Let $R = (\mathbb{Z}/3\mathbb{Z})[x]$. Consider the ideals $I_1 = (x^2 + 1)$, and $I_2 = (x^2 + x + 2)$ For $i = 1, 2$ we set $F_i = R/I_i$.

(a) Show F_1 and F_2 are fields.

(b) Are F_1 and F_2 isomorphic? If not why not, and if so give an isomorphism from F_1 to F_2.

Solution:

(a) Let $f(x) = x^2 + 1$ and $g(x) = x^2 + x + 2$. Note both are of degree 2, so will be irreducible if they have no roots in the ground field $\mathbb{Z}/3\mathbb{Z} = \mathbb{F}_3$. We compute directly: $f(0) = 1, f(1) = 2 = f(2)$, so $f(x)$ is irreducible, and $g(0) = 2, g(1) = 1, g(2) = 2$, so again $g(x)$ is irreducible. Since $\mathbb{F}_3$ is a field, R is a PID. Since $f(x)$ and $g(x)$ are both irreducible, and hence $(f(x))$ and $(g(x))$ are both maximal ideals in R. Thus, $F_1 = R/(f(x))$ and $F_2 = R/(g(x))$ are both fields.

(b) Both $F_1/\mathbb{F}_3$ and $F_2/\mathbb{F}_3$ are extensions of degree 2. Since there is a unique field of order 9, up to isomorphism, we know $F_1 \simeq F_2$. Note both F_1 and F_2 can be represented by elements $\{\overline{a+bx} | a, b \in \mathbb{F}_3\}$. However, the rules for multiplaction are different. Moreover, $f(x+2) = f(x-1) = (x-1)^2 + 1 = (x^2 - 2x + 1) + 1 = g(x)$. Therefore, the map $\varphi : F_1 \to F_2$ given by $\varphi(\overline{a+bx}) = \overline{a + b(x+2)} = \overline{(a+2b) + bx}$. is an isomorphism. $\square$

8. **(15 points)** Suppose F is a field, $K = F(\alpha)$ is a Galois extension, with cyclic Galois group generated by $\sigma : \alpha \mapsto \alpha + 1$. Show char $K = p \neq 0$, and $\alpha^p - \alpha \in F$.

Solution: Note, by induction we see, $\sigma^n(\alpha) = \alpha + n$ (since $\sigma^n(\alpha) = \sigma(\sigma^{n-1}(\alpha)) = \sigma(\alpha + (n-1)) = \alpha + 1 + n - 1 = \alpha + n$). Since K/F is Galois, hence finite, we have $\sigma^n = 1_K$, for some n. Therefore, if n is such an integer, then $\alpha = \sigma^n(\alpha) = \alpha + n$, so $n \cdot 1 = 0$, and hence char $F < \infty$. Thus, F has characteristic p, for some prime p. Also, since F has characteristic p,$\alpha^p(\alpha) = \sigma(\alpha)^p = (\alpha+1)^p = \alpha^p + 1^p = \alpha^p + 1$. Now $\sigma(\alpha^p - \alpha) = \sigma(\alpha^p) - \sigma(\alpha) = (\alpha^p + 1) - (\alpha + 1) = \alpha^p - \alpha$. Thus, $\alpha^p - \alpha \in K^{<\sigma>} = F$. $\square$