Algebra Qual Fall 2017

Problem 1

Statement (10 points)**.** Suppose the group G acts on the set A. Assume this action is faithful (recall that this means that the kernel of the homomorphism from G to $\mathrm{Sym}(A)$ which gives the action is trivial) and transitive (for all a, b in A, there exists g in G such that $g \cdot a = b$.)

(a) For $a \in A$, let G_a denote the stabilizer of a in G. Prove that for any $a \in A$, $\bigcap_{\sigma \in G} \sigma G_a \sigma^{-1} = 1$.

(b) Suppose that G is abelian. Prove that $|G| = |A|$. Deduce that every abelian transitive subgroup of S_n has order n.

Solution. **(a)** Recall that G acts faithfully if the only element that fixes everything in A is the identity. Equivalently if $\phi : G \to S_A$ is the corresponding morphism then

$$\ker \phi = \bigcap_{a \in A} G_a = \{e\}.$$

Now since the group action is transitive (only one orbit) all stabilizers are conjugate, thus

$$\bigcap_{\sigma \in G} \sigma G_a \sigma^{-1} = \bigcap_{a \in A} G_a = \{e\}$$

as desired.

(b) If G is abelian then conjugation is trivial i.e. $\sigma G_a \sigma^{-1} = G_a$. Then the intersection previous is just over one element so we may conclude $G_a = \{e\}$ for every $a \in A$. Then orbit stabilizer yields

$$|G| = |A| \cdot |G_a| = |A|$$

as desired.

That $G \leq S_n$ is transitive means that G acts transitively on $\{1, 2, \ldots, n\}$. Then this action is also faithful since the action of S_n is faithful. If $\sigma(m) = m$ for every $m \in [n]$ then its the identity permutation. Then parts (a) and the above yield

$$|G| = |[n]| = n.$$

Alternative solution

Recall that if G acts transitively on a set A then there is a G-set isomorphism $f : G/G_a \to A$ for any $a \in A$ defined by

$$f(gG_a) = g \cdot a.$$

Well defined: if $gG_a = g'G_a$ then $g = g'k$ for $k \in G_a$ and thus

$$f(gG_a) = g \cdot a = g' \cdot (k \cdot a) = g' \cdot a = f\left(g'G_a\right)$$

so the map is well defined.

Surjective: Since there is only one orbit for every $a' \in A$ there is $g \in G$ such that $g \cdot a = a'$. Then $f(gG_a) = a'$ and the map is surjective.

Injective: If $g \cdot a = g' \cdot a$ then $a = g^{-1}g' \cdot$ so $g^{-1}g' \in G_a$ and thus the cosets are equal.

G-equivariant: $g \cdot f(kG_a) = g \cdot (k \cdot a) = gk \cdot a = f(gkG_a)$.

Then this entire exercises becomes pretty trivial with this isomorphism.

Note that G_a is its stabilizer for the action on cosets G/G_a. Then if the action of G on G/G_a is free we must have $G_a = \{e\}$ and thus $G/G_a \cong G$. In other words the action is just G acting on itself by left multiplication. Then of course $|G| = |f(G)| = |A|$ so (b) is done as well. For the S_n claim the same argument is fine. □

Problem 2

Statement (15 points). **(a)** Classify the abelian groups of order 36.
For the rest of the problem, assume that G is a non-abelian group of order 36. (You may assume that the only subgroup of order 12 in S_4 is A_4 and that A_4 has no subgroup of order 6.)

(b) Prove that if the 2-Sylow subgroup of G is normal, G has a normal subgroup N such that G/N is isomorphic to A_4.

(c) Show that if G has a normal subgroup N such that G/N is isomorphic to A_4 and a subgroup H isomorphic to A_4 it must be the direct product of N and H.

(d) Show that the dihedral group of order 36 is a non-abelian group of order 36 whose Sylow-2 subgroup is not normal.

Solution. **(a)** By the fundamental theorem of finitely generated abelian groups we have that G is isomorphic to one of

$$C_2 \times C_2 \times C_3 \times C_3$$
$$C_4 \times C_3 \times C_3$$
$$C_4 \times C_9$$
$$C_2 \times C_2 \times C_9$$

(b) We claim the 3-sylow subgroup is not normal. Indeed if it was we would again have

$$G = P \rtimes Q.$$

If both are normal elements of P commute with elements of Q and since groups of order p^2 are abelian P and Q are both abelian from which we conclude G is abelian. Then the sylow 3-subgroup P is not normal and the 3rd sylow theorem yields $n_3 = 4$.

Now let G act on the set of 3-sylow subgroups by conjugation. Then this action induces a homorphism $\phi : G \to S_4$. Let $N = \ker\phi$. Since $|G| > |S_4|$ the map cannot be injective and N is non-trivial. Since the action is transitive it is not the trivial action so N is a proper normal

subgroup. We claim N has order 3. Indeed noting that the stabilizer of a 3-sylow is its normalizer and $n_3 = 4$ is the size of the single orbit we get

$$9 = \frac{|G|}{n_3} = |N_G(P)|, \text{ for each } P \text{ sylow subgroup.}$$

Then

$$N = \bigcap_{\text{3-sylow } P} N_G(P)$$

is a proper non trivial subgroup of a group of order 9 so it must have order 3. Then from the first isomorphism theorem

$$\frac{G}{N} \cong \operatorname{im} \phi$$

and $|G/N| = 12$ so the image has size 12. Of course the unique subgroup of S_4 of order 12 is A_4 so $G/N \cong A_4$.

Oh and N is normal since its a kernel.

(c) First we show $N \cap H = \{e\}$. Indeed suppose not. Since N has order 3 is simply a copy of C_3. Then if H contains any non-trivial elements of N is contains a generator, thus the entire group $N \subseteq H$. Then since N is normal in G its normal in H. Then by Cauchy's theorem H has an element of order 2 and thus a copy of C_2. Then since N and C_2 have coprime order $N \cap C_2 = \{e\}$ and we have a semidirect product $N \rtimes C_2 \subseteq H$ which has order 6. This contradicts that H has no subgroup of order 6.

Now $G = N \rtimes H$, (the order of this product is the order of the group so it must be the entire thing) and it remains to show this product is direct. Recall that N has order 3 thus its automorphism group $\operatorname{Aut}(N) = C_2$. I.e. there are only two automorphisms. The identity and $a \mapsto a^{-1}$.

Then consider the homomorphism for this semidirect product $\phi : A_4 \to C_2$. Now ϕ cannot be injective since $|A_4| > 2$. Then if ϕ is not the trivial map then its kernel must have order 6 contradicting that A_4 has no subgroup of order 6. Then ϕ is the trivial map and the semidirect product is direct.

(d) First D_{18} is not abelian by definition $sr = r^{-1}s$ and r is not self inverse since it has order 18. Then if the sylow 2 subgroup of D_{18} was normal by part (a) it would have a normal copy of C_3 such that $D_{18}/C_3 \cong A_4$.

Consider the image of $r \in A_4$. Since A_4 only has elements of order $2, 3$ we must have $r^6 C_3 = C_3$. But then $r^6 \in C_3$ is an element of order 3 so it must generate and we get $C_3 = \langle r^6 \rangle$. But then $D_{18}/\langle r^6 \rangle$ has a subgroup of order 6 namely the cosets represented by $\{e, r, r^2, r^3, r^4, r^5\}$. □

Problem 3

Statement (10 points)**.** Let F be a field. Let $f(x)$ be an irreducible polynomial in $F[x]$ of degree n and let $g(x)$ be any polynomial in $F[x]$. Let $p(x)$ be an irreducible factor (of degree m) of the polynomial $f(g(x))$. Prove that n divides m. Use this to prove that if r is an integer which is not a perfect square, and n is a positive integer then every irreducible factor of $x^{2n} - r$ over $\mathbb{Q}[x]$ has even degree.

Solution. Suppose α is a root of $p(x)$. Note that

$$F(\alpha) \cong \frac{F[x]}{\langle p(x) \rangle}$$

and this has degree m as an extension of F. Then since α is also a zero of $f(g(x))$ we see that $g(\alpha) \in F(\alpha)$ is a root of $f(x)$ in $F(\alpha)$. Then $F(g(\alpha)) \subseteq F(\alpha)$ and is isomorphic to $\frac{F[x]}{\langle f(x)\rangle}$ which has degree n over F. Then the tower law yields

$$m = [F(\alpha) : F] = [F(\alpha) : F(g(\alpha))] \cdot [F(g(\alpha)) : F] = [F(\alpha) : F(g(\alpha))]n.$$

Note that if $f(x) = x^2 - r$ then f is irreducible over $\mathbb{Q}$ since r is not a perfect square (the roots of f are $\sqrt{r}$ and this is not in $\mathbb{Q}$.) Then note that $x^{2n} - r = f(x^n)$, so by the above $\deg f = 2$ divides the degree of every irreducible factor. □

Problem 4

Statement (10 points). **(a)** Let $f(x)$ be an irreducible polynomial of degree 4 in $\mathbb{Q}[x]$ whose splitting field K over $\mathbb{Q}$ has Galois group $G = S_4$. Let θ be a root of $f(x)$. Prove that $\mathbb{Q}[\theta]$ is an extension of $\mathbb{Q}$ of degree 4 and that there are no intermediate fields between $\mathbb{Q}$ and $\mathbb{Q}[\theta]$.

(b) Prove that if K is a Galois extension of $\mathbb{Q}$ of degree 4, then there is an intermediate subfield between K and $\mathbb{Q}$.

Solution. **(a)** Note that

$$\frac{\mathbb{Q}[x]}{\langle f(x)\rangle} \cong \mathbb{Q}[\theta]$$

by the evaluation map. Then $\mathbb{Q}[x]/\langle f\rangle$ has a basis $1, x, x^2, x^3$ as a vector space over $\mathbb{Q}$ thus is dimension 4 (it is a field since f is irreducible.) Let $H^\theta = \mathrm{Gal}(K/\mathbb{Q}[\theta])$ be the subgroup whose fixed field is $\mathbb{Q}[\theta]$. Then by the Galois correspondence

$$[G : H^\theta] = [\mathbb{Q}[\theta] : \mathbb{Q}] = 4.$$

Then if H^θ has index 4 it must be order 6, and the only order 6 subgroups of S_4 are S_3.

Now suppose $\mathbb{Q} \subseteq E \subseteq \mathbb{Q}[\theta]$ is a proper non-trivial intermediate extension. Then

$$4 = [\mathbb{Q}[\theta] : \mathbb{Q}] = [\mathbb{Q}[\theta] : E][E : \mathbb{Q}].$$

Since $E \neq \mathbb{Q}, \mathbb{Q}[\theta]$ neither of these is 1 thus $[E : \mathbb{Q}] = 2$. Then again by the Galois correspondence the corresponding subgroup H^E must have index 2, thus order 12 i.e. $H^E = A_4$. But then also since $E \subseteq \mathbb{Q}[\theta]$ we have

$$S_3 = H^\theta \subseteq H^E = A_4$$

so S_3 is not a subgroup of A_4 so such an extension cannot exist.

(b) From the Galois correspondance $|\mathrm{Gal}(K/\mathbb{Q})| = [K : \mathbb{Q}] = 4$. Then the subgroups of order 4 are just C_4 and V_4 both of which have a proper subgroup C_2. Then the fixed field of C_2 will be an intermediate extension. □

Problem 5

Statement (10 points). A ring R is called simple if its only two-sided ideals are 0 and R.

(a) Suppose R is a commutative ring with 1. Prove R is simple if and only if R is a field.

(b) Let k be a field. Show the ring $M_n(k)$, $n \times n$ matrices with entries in k, is a simple ring.

Solution. **(a)** Suppose R is a field, and $I \subseteq R$ is a non-zero ideal. Then there is $a \in I \setminus \{0\}$. Since a is non-zero it is a unit. Then since I is an ideal

$$1 = a^{-1} \cdot a \in I$$

so that $r \cdot 1 = r \in I$ for all $r \in R$. Then $I = R$ as desired.

Conversely suppose the only ideals of R are $\{0\}$ and R. Then if $a \in R \setminus \{0\}$ consider the ideal generated by a. Since $(a) \neq (0)$ we must have $(a) = R$. Then $1 \in (a)$ so that $ax = 1$ for some $x \in R$. Then of course $x \in a^{-1}$.

(b) Suppose $J \subseteq M_n(k)$ is a non-zero ideal. Then there is $A \neq 0$ in J. Then A must have a non-zero row. WLOG suppose its the first one (other wise reorder the rows by multiplying by a permutation matrix on the left.) Then

$$\begin{bmatrix} 1 & & & \\ & 0 & & \\ & & \ddots & \\ & & & 0 \end{bmatrix} A = \begin{bmatrix} a_1 & a_2 & \cdots & a_n \\ & \ddots & & \\ & & \ddots & \\ & & & 0 \end{bmatrix} \in J$$

Then since this is a non-zero matrix it has a non-zero column. WLOG suppose its the first one (or reoder the columns.) Then we subtract $a_i a_1^{-1}$ times the first column from the ith column to zero the rest of the row. Then scaling by a_1^{-1} we obtain the matrix

$$E_{11} := \begin{bmatrix} 1 & & & \\ & 0 & & \\ & & \ddots & \\ & & & 0 \end{bmatrix} \in J$$

where by E_{ii} we mean the matrix with a 1 in the ith diagonal entry and 0's elsewhere. Then since $E_{11} \in I$ we can obtain E_{ii} by conjugating by the permutation matrix $t_{1,i}$ that swaps row 1 with row i when multiplying on the left and swaps column 1 with column i when multiplying from the right. Then

$$I = E_{11} + E_{22} + \cdots + E_{nn} \in J$$

thus $J = M_n(k)$ since it contains the identity.

Remark. The subtraction matrices you need for the columns are the same as the matrices you use the subtract rows from rows. You just multiply on the right instead of the left. These are things like

$$\begin{bmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \qquad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 0 & 1 \end{bmatrix}$$

which are matrices which tract the 1st column from the 2nd or the 3rd.

□

Problem 6

Statement (15 points)**.** For a ring R, let $U(R)$ denote the multiplicative group of units in R. Recall that in an integral domain R, $r \in R$ is called irreducible if r is not a unit in R, and the only divisors of r have the form ru with u a unit in R. We call a non-zero, non-unit $r \in R$ prime in R if $r \mid ab$ implies $r \mid a$ or $r \mid b$. Consider the ring $R = \left\{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\right\}$.

(a) Prove R is an integral domain.

(b) Show $U(R) = \{\pm 1\}$.

(c) Show 3, $2 + \sqrt{-5}$, and $2 - \sqrt{-5}$ are irreducible in R.

(d) Show 3 is not prime in R.

(e) Conclude R is not a PID.

Solution. **(a)** R is subset of $\mathbb{C}$, and subrings of domains are domains so R is a domain.

(b) Recall we have a norm on R given by

$$N\left(a + b\sqrt{-5}\right) = \left(a + b\sqrt{-5}\right)\left(a - b\sqrt{-5}\right) = a^2 + 5b^2 \in \mathbb{N}.$$

Then if $\alpha \in R$ is a unit

$$1 = N(1) = N\left(\alpha \cdot \alpha^{-1}\right) = N(\alpha)\, N\left(\alpha^{-1}\right)$$

Then we must have $N(\alpha) = N\left(\alpha^{-1}\right) = 1$. Now consider that if

$$a^2 + 5b^2 = 1$$

we must have $b = 0$ since otherwise the norm is at least 5. Then $a^2 = 1$ so $a = \pm 1$ and these are the only units in R as desired.

(c) Note that all of these elements have norm 9. Then it suffices to show that any element of norm 9 is irreducible. Indeed suppose $\alpha\beta$ has norm 9 and neither of α, β is a unit (equivalently neither is ± 1.) Then we have

$$9 = N(\alpha\beta) = N(\alpha)\, N(\beta)$$

and since neither is 1 neither can be 9 so we must have $N(\alpha) = N(\beta) = 3$. Then consider that if

$$a^2 + 5b^2 = 3$$

we again must have $b = 0$. Then $a^2 = 3$ has no solutions in $\mathbb{Z}$. Then α, β cannot exist and every element of norm 3 is irreducible.

(d) Note that $3 \mid 9$, but 3 does not divide either of $2 + \sqrt{-5}$ or $2 - \sqrt{-5}$. Then note

$$9 = N\left(2 + \sqrt{-5}\right) = \left(2 + \sqrt{-5}\right)\left(2 - \sqrt{-5}\right).$$

(e) The above shows R is not a UFD, and since PID's are UFDs R cannot be a PID. Alternatively we can consider the ideal generated by

$$\left(3, 2 + \sqrt{-5}\right).$$

If this was principle then 3 and $2 + \sqrt{-5}$ would have a common divisor. But they are irreducible thus have no non-trivial divisors. □

Problem 7

Statement (15 points)**.** Let F be a field and let V and W be vector spaces over F. Make V and W into $F[X]$-modules via linear operators T on V and S on W by defining $X \cdot v = T(v)$ for all $v \in V$ and $X \cdot w = S(w)$ for all $w \in W$. Denote the resulting $F[X]$-modules by V_T and W_S respectively.

(a) Show that an $F[X]$-module homomorphism from V_T to W_S consists of an F-linear transformation $R : V \to W$ such that $RT = SR$.

(b) Show that $V_T \cong W_S$ as $F[X]$-modules if and only if there is an F-linear isomorphism $P : V \to W$ such that $T = P^{-1}SP$.

(c) Recall that a module M is simple if $M \neq 0$ and any proper submodule of M must be zero. Suppose that V has dimension 2. Give an example of F, T with V_T simple.

(d) Assume F is algebraically closed. Prove that if V has dimension 2, then any V_T is not simple.

Solution. **(a)** Suppose $R : V_T \to W_S$ is an isomorphism of $F[x]$-modules. Then R is additive

$$R(u+v) = R(u+v)$$

and since it commutes with the action of polynomials, and $a \in F$ is simply a constant polynomial it commutes with scalars as well $R(au) = aR(u)$. Then R is simply a linear map that commutes with the action of $x \in F[x]$. Now for any $v \in V$ we have

$$RTv = R(x \cdot v) = x \cdot Rv = SRv$$

hence $RT = SR$ since they agree on all vectors.

(b) Suppose the above R is an isomorphism. Then it has an inverse R^{-1}. Then $RT = SR$ implies $RTR^{-1} = S$.

Conversely suppose there is such an invertible $R : V \to W$. Then R is precisely a linear map that commutes with the action of x. That is $RT = SR$ is equivalent to $R(x \cdot v) = x \cdot R(v)$. Then R lifts to a map of $F[x]$-modules, and since it is invertible it is an isomorphism.

(c) We can read this as saying that it has dimension 2 as a vector space over F, but as an $F[x]$ module it is simple,

This is related to cyclic i.e. generated by a single element. We actually went through a problem recently showing that this can only happen if there is a linear operator A and a vector V such that v, Av are independent, and that this happens iff the minimal polynomial of that operator is equal to the characteristic polynomial.

Then this interpretation motivates picking a matrix who's charpoly is its minpoly (so we get a cyclic module) and is irreducible (so we get a field.) Consider

$$T = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \in M_2(\mathbb{R}).$$

Then $\dim \mathbb{R}^2 = 2$ as an $\mathbb{R}$ vector space, but as an $\mathbb{R}[x]$-module it is isomorphic to (using the fundamental theorem of f.g modules over a PID primary form)

$$\mathbb{R}^2 \cong \frac{\mathbb{R}[x]}{\langle x^2+1 \rangle}, \text{ where } x^2+1 = \chi_T(x) = M_T(x).$$

Then x^2+1 is irreducible in $\mathbb{R}[x]$ (it has no roots there) so it is a field thus simple as a $\mathbb{R}[x]$-module (the submodules are ideals and this has none.)

(d) Suppose F is algebraically closed. Then the characteristic polynomial of T factors as

$$\chi_A(x) = (x - w_0)(x - w_1), w_i \in F.$$

Then if $w = w_0 = w_1$ then as an $F[x]$-module using primary form of classification we get

$$V \cong \frac{F[x]}{\left\langle (x-w)^2 \right\rangle}, \text{ or } V \cong \frac{F[x]}{\langle x - w \rangle} \oplus \frac{F[x]}{\langle x - w \rangle}$$

Then the first ring has the non-zero proper submodule $\langle \overline{x - w} \rangle$, and the second each non-zero added is a proper submodule. Instead if the roots are distinct then

$$V \cong \frac{F[x]}{\langle x - w_0 \rangle} \oplus \frac{F[x]}{\langle x - w_1 \rangle}$$

as a $F[x]$-module. Then each addend is a non-zero submodule. □