MATH 3340 FINAL WITH ANSWERS, SPRING 2017

1. Let $H \leq G, N \leq G$ be two subgroups of a finite group G. Define a function $\phi : H \times N \to G$ by $(h, n) \mapsto hn$.

a. Prove that the size of the image is $\frac{\#H\ \#N}{\#(H\cap N)}$.

Answer. The source $H \times N$ is of size $\#H\ \#N$, and the image must be smaller or equal to that in size. So somehow the failure of ϕ to be $1 : 1$ is getting measured by $H \cap N$.

Let's look at the sizes of the equivalence classes given by $(h_1, n_1) \sim (h_2, n_2)$ if $\phi(h_1, n_1) = \phi(h_2, n_2)$, i.e. $h_1 n_1 = h_2 n_2$, or $h_2^{-1} h_1 = n_2 n_1^{-1}$. This $h_2^{-1} h_1 = n_2 n_1^{-1}$ is in both H and N, i.e. is in $H \cap N$.

Put another way, $(h_1, n_1) \sim (h_2, n_2)$ iff $(h_1, n_1) = (h_2 k, k^{-1} n_2)$ for some unique element $k \in H \cap N$. So all the equivalence classes are of the same size, $\#(H \cap N)$.

[Note that it's NOT okay to just assume ϕ is a homomorphism and compute the kernel – in part 1d below, it's not a homomorphism! If you carelessly decide the "kernel" of this ϕ is $\{(h, n)\ :\ \phi(h, n) = e\}$, you get the set $\{(k, k^{-1})\ :\ k \in H \cap N\}$, which may not even be a subgroup.]

1b. Find and prove a necessary and sufficient condition for ϕ to be a homomorphism.

Answer. $\phi((h_1, n_1)(h_2, n_2)) = \phi((h_1 h_2, n_1 n_2)) = h_1 h_2 n_1 n_2$, but if it's a homomorphism then that's supposed to also be $\phi(h_1, n_1)\phi(h_2, n_2) = h_1 n_1 h_2 n_2$. These are only always equal if $h_2 n_1 = n_1 h_2$ for all $h_2 \in H, n_1 \in N$, i.e. if H and N commute with each other.

[In particular, under this condition $H \cap N$ is abelian, which fits with the calculation of the "kernel" from before, now honestly the kernel.]

1c. If N is normal, prove that the image is a subgroup. (Do *not* assume your condition from 1b holds.)

Answer. We need to check closure under multiplication.

$$\phi(h_1, n_1)\phi(h_2, n_2) = h_1 n_1 h_2 n_2 = h_1 h_2 n' n_2 = \phi(h_1 h_2, n' n_2)$$

where $n' = h_2^{-1} n_1 h_2$ is in N by the assumption that it's normal.

1d. Give an example of a triple (H, N, G) where the image is *not* a subgroup.

Answer. To make 1c fail we need H, N to not be normal subgroups. To make 1b fail we need them to not commute with each other. So let's try $H = \langle (12) \rangle, N = \langle (23) \rangle$ inside S_3. By 1a, the image is of size 4, which doesn't divide $\#S_3$ so can't be a subgroup.

---

2. Let $R = \mathbb{Z}[i] \leq \mathbb{C}$, i.e. $i^2 = -1$. Let $I := \langle 3 \rangle$.

a. Find an element of R/I whose fourth power is not 0 or 1.

Answer. The elements can be written, modulo I, as $a + bi$ where $a, b \in \mathbb{Z}/3\mathbb{Z}$. Let's try $1 + i$ (since $0, 1, i$ all obviously don't work). Its powers are

$$1 + i, \quad 2i, \quad 2i + 1, \quad 2, \quad 2 + 2i, \quad i, \quad i + 2, \quad 1$$

so it's of order 8 in the group of invertible elements. In particular, the 1st, 3rd, 5th, 7th elements of that last are the possible answers.

2b. Prove that $I := \langle 3 \rangle$ is a prime ideal.

Answer. Or equivalently, that the quotient has no zero divisors. We just listed the nonzero elements (as powers of $1 + i$), and products of two powers are again on that same list, so the products are never 0.

2c. Prove that $J := \langle 5 \rangle$ is not a prime ideal.

Answer. $5 = (2 + i)(2 - i)$

---

3. Let $\tau = \exp(2\pi i/n) \in \mathbb{C}$ be a primitive nth root of unity.

a [10]. Prove that $Gal(\mathbb{Q}[\tau]/\mathbb{Q})$ is abelian.

Answer. Every automorphism is given by τ mapping to another nth root of unity, i.e. a power of τ. If we call that map ϕ_k taking $\tau \mapsto \tau^k$, then obviously $\phi_k \phi_m = \phi_{km} = \phi_m \phi_k$.

3b [10]. Let $F \leq \mathbb{Q}[\tau]$ be a subfield. Prove that $Gal(F/\mathbb{Q})$ is abelian.

Answer. We showed that if S is a splitting field (as in this case), and $S \geq F \geq E$, then $Gal(F/E)$ is a quotient of the subgroup $Stab(F) \leq Gal(S/E)$. (Here $Stab(F) = \{\sigma \in Gal(S/E) : \sigma(F) = F\}$.)

Now use: a subgroup of an abelian group is abelian, and a quotient of an abelian group is abelian.

---

4. Let I, J be ideals in a commutative ring R, and define

$$I : J \quad := \quad \{r \in R \mid rJ \leq I\}$$

Prove that $I : J$ is an ideal.

Answer. If $r \in I : J$ and $s \in R$, then $srJ \leq sI \leq I$, so $sr \in I : J$ too.

---

5. Let $\pi \in S_{a+b}$ be the permutation $(1\ 2\ \cdots\ a)(a{+}1\ a{+}2\ \cdots\ a{+}b)$. How many disjoint cycles does π^k have, for each k?

Answer. The first cycle breaks into $gcd(a, k)$ cycles, the second into $gcd(b, k)$ cycles, for a total of $gcd(a, k) + gcd(b, k)$.

---

6 [10]. Let $F \geq \mathbb{Q}$ be the splitting field of some polynomial $b(x)$.
Show that there exists an element $f \in F$ such that $F = \mathbb{Q}[f]$.

Answer. We showed that if $E \leq F$ is an intermediate field, and $Gal(F/E) \leq Gal(F/\mathbb{Q})$ is the subgroup of field automorphisms leaving every $e \in E$ in place, then $F^{Gal(F/E)} = E$. Hence to every subfield, we can associate a subgroup of $Gal(F/\mathbb{Q})$, in a $1 : 1$ fashion.

We showed that F is a finite extension, so its Galois group is finite, hence has finitely many subgroups. Putting that and the previous paragraph together, there are only finitely many "proper" subfields (meaning, not the whole thing).

Since $\mathbb{Q}$ is infinite and F is a vector space over $\mathbb{Q}$, it's not the union of finitely many proper subspaces. So there exists an element $f \in F$ that's not in any of those proper subfields.

Now $\mathbb{Q}[f] \leq F$ is a subring, hence a domain, hence (being finite-dimensional over $\mathbb{Q}$) a field. So it's a subfield, but not a proper subfield, so it's the whole thing.

---

7 [10]. Let $X = \{n \in \mathbb{N} \,:\, n \geq 4\}$.
Define a relation $R := \{(a, b) \in X \times X \,:\, b \text{ is an integer multiple of } a\}$.
Let $\sim \supseteq R$ be the equivalence relation generated by R.

How many equivalence classes are there in $X/{\sim}$?

Answer. For any two $m, n \in X$, we have mn is a multiple of m, and of n. So $m \sim mn \sim n$. Hence everybody's equivalent to everybody else, i.e. there's only one equivalence class.